# Product Security Baseline
# Linux Distribution Requirements

## Version 1.0

# Contents

# 1 Introduction

This document seeks to assist Cisco product teams in formulating plans for the acquisition of Linux OS distributions. To achieve this, this document specifies a set of security requirements that is intended to be applicable across all Linux distributions. Product teams can use the requirements to validate or improve the security stance of the base OS, thus providing a more secure foundation to layer on application specific features. The requirements draw from a number of sources, including but not limited to:

- Cisco's internal security requirements based on our observations in security trends and exploit mitigation strategies.
- Security Technology Implementation Guide (STIG) UNIX version 5.0 r1.
- Common Criteria Operation System Protection Profile (OSPP) version 2.0.
- A Profile for IPv6 in the U.S. Government (USGv6) version 1.0.

This document does not contain Cisco proprietary information, and can be shared with third party Linux vendors.

The initial version of this document primarily focus on requirements for embedded Linux distributions, application stack level requirements will be added in subsequent versions. Additionally, attempts have been made to separate Linux specific information in the requirements. Typically, Linux specific guidelines would be included as "*Application Note*", similar to the approach taken in Common Criteria protection profile specifications. If a product team chose to leverage a non-Linux based OS, it should be fairly trivial to remove all Linux specific information, and reuse this document as a security baseline for the OS under evaluation.

The terminology used to describe requirements in this document include: "mandatory", "optional" (with their common meaning), and "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" which are to be interpreted as described in RFC 2119.

# 2 Requirements Summary

The following table summarizes all of the requirements in this document. Section 3 to 9 describes the requirements in more detail.

| Priority | Req Name | Req Description |
|---|---|---|
| | Robustness and Resiliency | |
| Required | SEC-ASLR-SCOPE | ABILITY TO RANDOMIZE ALL CODE AND DATA (ASLR) |
| Required | SEC-ASLR-CONFIG | ASLR IMPLEMENTATION MUST USE STANDARD CONFIG |
| Required | SEC-ASLR-DIST | RANDOMIZE PROCESSES THAT ARE PART OF DISTRIBUTION |

| | | |
|---|---|---|
| Recommended | SEC-ASLR-RND | USE SECURE RANDOM NUMBER GENERATION |
| Required | SEC-ASLR-RANGE | SUFFICIENT NUMBER OF POTENTIAL RANDOMIZED LOCATIONS |
| Required | SEC-NX-SCOPE | ABILITY TO MUTUALLY EXCLUDE WRITE AND EXECUTE PAGES (NX BIT) |
| Required | SEC-NX-DIST | MUTUALLY EXCLUDE WRITE AND EXECUTE PAGES FOR PROCESSES THAT ARE PART OF DISTRIBUTION |
| Required | SEC-BE-STABLE | REMAIN STABLE DURING FLOODING ATTACK |
| | DISPLAY, LOGGING AND AUDITING | |
| Required | SEC-ALL-LOGD-2 | SUPPORT LOGGING OF ALL MAJOR SYSTEM EVENTS |
| Required | SEC-CHG-LOGD-3 | LOG ALL CHANGES TO LOGGING CONFIGURATIONS |
| Required | SEC-AUD-FIELD-3 | INCLUDE IDENTIFYING INFORMATION IN ALL AUDIT RECORDS |
| Required | SEC-LIM-MESS | RATE LIMIT OR AGGREGATE AUDIT MESSAGES |
| Required | SEC-DSP-PROC | DISPLAY ACTIVE TCP/IP SERVICES (INCL. OPEN PORTS) |
| | ACCESS CONTROL AND PERMISSIONS | |
| Required | SEC-RFM-INST | SUPPORT COMPREHENSIVE ACCESS CONTROL POLICIES |
| Required | SEC-CRE-NOBACK | NO “BACK DOORS” |
| Required | SEC-DEF-PERM | MAINTAIN SECURE DEFAULT PERMISSIONS |
| Required | SEC-CRE-ROOT | MAINTAIN CAREFUL CONTROL OVER ROOT ACCOUNT |
| Required | SEC-DEF-SVC | DISABLE UNNECESSARY SERVICE TO REDUCE ATTACK SURFACE |
| | CREDENTIALS | |
| Recommended | SEC-LOG-INDC | INDICATE PASSWORD STATUS AT LOGIN |
| Recommended | SEC-BAN-BEFR-2 | ABILITY TO DISPLAY CONFIGURABLE BANNER BEFORE LOGIN |
| Recommended | SEC-BAN-AFTR-2 | ABILITY TO DISPLAY CONFIGURABLE BANNER AFTER LOGIN |
| Required | SEC-INC-USER | DO NOT DISCLOSE USERNAME VALIDITY ON FAILED LOGIN |
| Recommended | SEC-NUM-SESS-2 | LIMIT THE NUMBER OF CONCURRENT SESSIONS FOR ONE USER |
| Required | SEC-IDL-TMOUT-2 | ENFORCE IDLE SESSION TIMEOUT |
| Required | SEC-DEF-CRED-2 | NO WEAK INBOUND CREDENTIALS EXCEPT IN CLEAN STATES |
| Required | SEC-INT-CRED-2 | DISABLE WEAK INSTALLATION CREDENTIALS AFTER INSTALL |
| Required | SEC-NRCV-CRED-4 | HASH NON-RECOVERABLE STORED CREDENTIALS |
| Required | SEC-USR-FAIL | HANDLE FAILED LOGIN APPROPRIATELY |
| Required | SEC-USR-MESS | LOG ONLY VALID USERNAMES FOR FAILED LOGIN ATTEMPTS |
| Required | SEC-PWD-AUDIT | NEVER LOG PASSWORDS |
| Required | SEC-RES-LOSS-2 | RECOVER FROM LOSS OF AUTHENTICATION CREDENTIALS |
| Required | SEC-ERA-DATA-2 | SUPPORT CREDENTIAL LOSS RECOVERY VIA CLEAN STATE |
| Required | SEC-CRE-REST-2 | ENFORCE PASSWORD COMPLEXITY |
| Required | SEC-SUP-CHAR-2 | SUPPORT ALL STRUCK ASCII CHARACTERS IN PASSWORDS |
| Recommended | SEC-MIN-INTV | ABILITY TO ENFORCE MINIMUM END-USER PASSWORD CHANGE INTERVAL |
| Recommended | SEC-PWD-REUSE | RESTRICT END-USER PASSWORD REUSE |
| Recommended | SEC-CHG-INTV | ENFORCE MAXIMUM END-USER PASSWORD LIFETIME |
| Required | SEC-PWD-CHECK | RESTRICT PASSWORDS ONLY AT PASSWORD CHANGE |
| Recommended | SEC-CHG-PSWD-2 | AUTHENTICATE AT PASSWORD CHANGES |

| | PROTOCOL | |
|---|---|---|
| Required | SEC-OFF-PROC | SELECTIVELY ENABLE TCP/IP SERVICES (INCL. OPEN PORTS) |
| Recommended | SEC-WEL-PORT-2 | DON'T RUN THE WRONG PROTOCOLS ON WELL-KNOWN PORTS |
| Required | SEC-CON-PERM | FILTER INCOMING CONNECTIONS BY SOURCE IP ADDRESS |
| Required | SEC-LIM-TRAF | CONFIGURABLY RATE-LIMIT IP BASED ON LAYERS 3 AND 4 |
| Required | SEC-TCP-RAND | RANDOMIZE INITIAL TCP SEQUENCE NUMBERS |
| Recommended | SEC-ARP-STAT-2 | SUPPORT STATIC IP-TO-MAC ADDRESS BINDINGS |
| Required | SEC-SSH-V2.0 | SUPPORT SSH V2 |
| Required | SEC-DHCP-RAND | RANDOMIZE DHCP TRANSACTION ID FIELDS |
| Required | SEC-TIME-NTP | USE NTP FOR DATE AND TIME MAINTENANCE |
| Required | SEC-NTP-IPFILT | SEPARATELY FILTER NTP PEERS AND CLIENTS BY IP ADDRESS |
| Required | SEC-NTP-AUTH3 | SUPPORT NTPV3 AUTHENTICATION |
| Required | SEC-NTP-AUTH4 | SUPPORT NTPV4 AUTHENTICATION |
| Required | SEC-SNM-AES | SUPPORT AES-128 FOR SNMPV3 |
| Required | SEC-SNM-SHA96 | HMAC-SHA-96 FOR SNMPV3 AUTHENTICATION |
| Required | SEC-HTP-SSL3-2 | SUPPORT TLS AND NEGOTIATE SSLV3 FOR HTTP |
| Required | SEC-IPS-ESP-3 | SUPPORT IPSEC ESP ENCRYPTION FOR ALL UNICAST IP |
| Required | SEC-IP-IPV6 | SUPPORT ALL SECURITY REQUIREMENTS OVER IPV6 |
| Required | SEC-IPV6-LMT | ABILITY TO SET UPPER BOUND ON IPV6 PREFIX LIST AND RECONFIGURATION |
| Recommended | SEC-IPV6-SEND | IMPLEMENT IPV6 SECURE NEIGHBOR DISCOVERY PROTOCOL (SEND) |
| Recommended | SEC-IPV6-CGA | IMPLEMENT IPV6 CRYPTOGRAPHICALLY GENERATED ADDRESS |
| Required | SEC-IPV6-USGV6 | IPV6 IMPLEMENTATION MUST BE USGV6 COMPLIANT |
| Required | SEC-DNS-DNSSEC | FULLY SUPPORT DNSSEC FOR ALL DNS APPLICATIONS |
| | CRYPTO | |
| Required | SEC-KER-FIPS | KERNEL CRYPTO MODULE MUST BE FIPS 140-2 CERTIFIED |
| | TOOLCHAIN AND PROCESS | |
| Required | SEC-RUN-OSC | PROVIDE SUPPORT FOR OBJECT SIZE CHECKING (BOSC) |
| Required | SEC-RUN-PROP | PROVIDE SUPPORT FOR STACK SMASHING PROTECTION |
| Required | SEC-RUN-SA | RUN STATIC ANALYSIS AND FIX HIGH PRIORITY SECURITY DEFECTS |
| Required | SEC-SUP-SFT | PROVIDE INVENTORY OF ALL USER SPACE CODE |
| Required | SEC-SUP-SRC | PROVIDE SOURCE CODE FOR TOOLCHAIN |
| Required | SEC-SUP-PATCH | SECURITY INCIDENT NOTIFICATION AND RESPONSE |
| Recommended | SEC-CERT-STIGS | RECEIVE UNIX OR RED HAT STIGS CERTIFICATION |
| Recommended | SEC-CERT-CC | RECEIVE COMMON CRITERIA CERTIFICATION |

# 3 Robustness and Resiliency

### SEC-ASLR-SCOPE - Ability to randomize all Code and Data (ASLR)

OS MUST provide ability to randomize all program and data locations. This requirement includes randomization of following sections of a program:

- Stack
- Heap
- Main Program
- Shared Library / mmap()
- Virtual Dynamic Shared Object (VDSO)

*Application Note: On Linux, Address Space Layout Randomization (ASLR) was introduced in version 2.6.12 with x86 architecture focus. Subsequent releases of the kernel incrementally added additional ASLR functionalities. For example, heap randomization was added for x86 in 2.6.25, and for ARM in 2.6.37. At time of drafting this requirement, 2.6.37 represents the minimal acceptable kernel version. It contains full ASLR support for x86 and ARM architecture, and acceptable level of ASLR support for PowerPC and MIPS architecture.*

### SEC-ASLR-CONFIG – ASLR implementation must use standard config

The Linux Kernel ASLR implementation MUST use the following standard configuration options:

- A user-accessible toggle MUST be offered via the file /proc/sys/kernel/randomize_va_space.
- The contents of this file SHALL be viewed by running:

  *cat /proc/sys/kernel/randomize_va_space*

  or:

  *sysctl kernel.randomize_va_space*
- The possible values of randomize_va_space are:
  - 0: ASLR is disabled.
  - 1: All supported forms of ASLR are enabled, except heap randomization.
  - 2: All supported forms of ASLR are enabled.

The active level of ASLR applied to new programs can be changed by modifying the value of *randomize_va_space*, which can be done by running:

*sysctl -w kernel.randomize_va_space=NEWVALUE*

This must be run as root-privileged user, and changes will only affect programs started after the value is changed.

### SEC-ASLR-DIST - Randomize processes that are part of distribution

All processes that are as part of the OS distribution MUST be randomized.

*Application Note: This implies user space code must be built as Position Independent Executable (PIE), or –fPIE option in GCC.*

### SEC-ASLR-RND - Use Secure Random Number Generation

OS SHALL use a cryptographically secure pseudorandom number generator (CSPRNG) meeting either FIPS 186-2 or NIST SP 800-90 standards as the basis for determining the random offset for program code and data.

| | |
|---|---|
| NIST SP 800-90 | Recommendation for Random Number Generation Using Deterministic Random Bit Generators |
| FIPS 186-2 | Digital Signature Standards |

### SEC-ASLR-RANGE - Sufficient number of potential randomized locations

The ASLR implementation MUST select from at least 256 random locations for each of the memory segment specified in SEC-ASLR-SCOPE.

### SEC-NX-SCOPE - Ability to mutually exclude write and execute pages (NX bit)

OS MUST provide ability to disable writes to program and library machine code text segments, and to any data segments designated read-only by any object file being loaded, as soon as the contents of those segments have been loaded. Operating systems MUST by default disable CPU execution of data in writeable segments, including stacks and heaps.

### SEC-NX-DIST - Mutually exclude write and execute pages for processes that are part of distribution

All processes that are as part of the OS distribution MUST not run with both execute and write permissions on same memory pages.

*Application Note: This implies user space code must be built with flag PT_GNU_STACK enabled in the elf header.*

### SEC-BE-STABLE - Remain stable during flooding attack

OS MUST survive common flooding-based denial of service attacks (IPv4, IPv6).

- Continue to operate without reloading its software, including performing its ESSENTIAL functions, albeit perhaps with greatly reduced performance.
- Maintain the integrity and consistency of its internal data structures
- Recover gracefully, without human intervention, after the attack.

At a minimum, the OS MUST be remain stable during the following types of attacks

- A flood of 16KB fragmented IP datagrams, with the initial fragment of each datagram omitted, directly at the IP address of the machine. The source address and IP ID of each fragmented datagram MUST be different. These datagrams MUST be fragmented to the MRU of the receiving interface, except that if the MRU of the receiving interface is greater than or equal to 8KB, the datagrams MUST instead be fragmented such that each one is broken into at least three fragments (one of which will be missing from the data stream).
- A ping flood to the IP address of the machine
    - With datagrams of the minimum legal size for the input interface.
    - With 64KB ICMP echo datagrams fragmented to the MRU of the input interface. If the MRU of the input interface is greater than or equal to 32KB, the datagrams MUST instead be fragmented such that each one is broken into at least three fragments.

  All ping flood datagrams MUST use valid IP source addresses reachable by the OFFERING. The same source address MAY be used for each datagram.
- A SYN flood directed to a listening TCP port on the machine. Source addresses for SYN floods MUST be random syntactically valid IP addresses, independently chosen for each datagram.

# 4 Display, Logging and auditing

### SEC-ALL-LOGD-2 - Support logging of all major system events

OS MUST provide support to log all major system events. At a minimum, the OS must be capable of audit logging the following events:

- Service startup/shutdown, interruption, and resumption
- Modification to system time
- System startup/shutdown
- Failed attempts to access files and programs
- File deletions
- Account creation, deletion, and privilege modifications

- Login, logout, failed login attempt, and session initiation
- Discretionary access control permission modifications
- Loading and unloading of dynamic kernel modules

Please see requirement SEC-CHG-LOGD-3 on additional requirements for the logging service itself.

### SEC-CHG-LOGD-3 - Log all changes to logging configurations

Whenever any form of logging is in operation, all changes to the configuration of the logging service itself MUST be logged. Changes to the configuration of the logging service includes:

- Enabling or disabling logging
- Changes in logging servers or other log data destinations
- Changes to the logging protocols or to the configurations of those protocols
- Changes in system wide logging filters
- Changes to the logging severity or priority assigned to logging-related events such as loss of log data
- Changes to the system's response to the exhaustion of logging resources (such as disk full), changes in the sizes of logging buffers

If the logging configuration can be changed without the change itself being recorded, the integrity of logs can easily be compromised.

### SEC-AUD-FIELD-3 - Include identifying information in all audit records

Audit records need to say who or what did something, when they did it, what they did, and whether they succeeded. Each log message or audit record MUST include at least the following information:

- The date and time of the event, including time zone. The time MUST be taken from the internal clock of the device detecting the event. The logging or auditing server SHOULD additionally record its own time stamp for the received log record.
- The identity of the “subject” (username, process id, ip address, etc) provoking the event.
- The type and nature of the event.
- The outcome of the event. In particular, if the event was a request for some action, it MUST be possible to determine from the audit message whether the action succeeded or failed.

### SEC-LIM-MESS - Rate limit or aggregate audit messages

OS MUST provide the capability to rate limit or aggregate audit messages. If possible, rate limiting SHOULD be applied to individual sources of logging data and/or to individual event types, in addition to rate limiting logging as a whole. Rate limiting can also take the form of ability to rotate audit logs on a periodic basis (ie., daily).

### SEC-DSP-PROC - Display active TCP/IP SERVICEs (incl. OPEN PORTs)

The ADMINISTRATOR's user interface MUST be able to show a complete, unified list of all currently active TCP/IP SERVICEs. The list MUST include at least the following information:

1. The identity of LISTENER associated with each TCP/IP SERVICE
2. The IP addresses, ports, and/or IP protocol numbers for which each TCP/IP SERVICE is configured to respond.

## 5 Access Control and Permissions

### SEC-RFM-INST – Support comprehensive access control policies

OS MUST Include SELinux features in the kernel to support access control security policies (ie., Mandatory Access Control), through the use of Linux Security Modules (LSM).

### SEC-CRE-NOBACK - No "back doors"

OS MUST NOT include "back doors" for access by anyone, for any purpose, including "legitimate" service or support. This includes any form of access whatsoever, ADMINISTRATIVE or otherwise, by any person, employee or otherwise.

A back door is any means of access, or any means of increasing the control, information or resources available with some preexisting form of access, which is an intentional part of an OS or its implementation, and is not disclosed to anyone.

Any access or administrative capabilities that are enabled by default, including password recovery/reset, must be openly documented by the vendor. This includes, but is not limited to:

- User accounts in the base OS (e.g. via telnet/SSH)
- Accounts in the applications that constitute the product's functionality (e.g. via web UI, SNMP)
- Any available hidden services, or hidden modules/capabilities within known services.

### SEC-DEF-PERM – Maintain secure default permissions

OS MUST ensure default permission to critical system files, directories and other resources are set appropriately. The following table summarizes the requirements (mainly drawn from STIG UNIX version 1.0) for common resources. All resources listed MUST NOT use extended ACL.

| Resource | Owned | Group-owned | Mode |
|---|---|---|---|
| system audit logs | root | root,bin,sys,or system | 0640 |
| root account's home directory (other than /) | root | root | 0700 |
| time synchronization configuration file (such as /etc/ntp.conf) | root | root, bin, sys, or system | 0640 |
| network services daemon files | | | 0755 |
| system command files | system account | system group | 0755 |
| system log files | | | 0640 |
| library files | | | 0755 |
| NIS/NIS+/yp files | root, sys, or bin | root, sys, bin, other, or system | 0755 |
| /etc/resolv.conf file<br>/etc/hosts file<br>/etc/nsswitch.conf file<br>/etc/passwd file<br>/etc/group file | root | root, bin, sys, or system | 0644 |
| /etc/shadow file | root | root, bin, sys, or system | 0400 |
| user home directories | respective user | owner's primary group | 0750 |
| files and directories contained in user home directories | | group of which the home directory's owner is a member | |
| run control scripts | | | 0755 |
| system start-up files | root | root, sys, bin, other, or system | |
| global initialization files | root | root, sys, bin, other, system or the system default | 0644 |
| skeleton files (typically those in /etc/skel) | root or bin | root, bin, sys, system, or other | 0644 |
| local initialization files | user or root | user's primary group or root | 0740 |
| shell files | root or bin | root, bin, sys, or system | |
| public directories | root or an application account | root or an application group | |
| cron.allow | root, bin, or sys | root, bin, sys, or cron | 0600 |
| crontab files | | | 0600 |

| | | | |
|---|---|---|---|
| files in cron script directories | | | 0700 |
| cron and crontab | root or bin | root, sys, bin or cron | 0755 |
| cronlog | | | 0600 |
| cron.deny | root, bin, or sys | root, bin, sys, or cron | 0700 |
| at.deny | root, bin, or sys | root, bin, sys, or cron | 0600 |
| at.allow | root, bin, or sys | root, bin, sys, or cron | |
| "at" directory | root, bin, or sys | root, bin, sys, or cron | 0755 |
| traceroute command | root | sys, bin, root, or system | 0700 |
| alias file | root | root, sys, bin, or system | 0644 |
| snmpd.conf | root | root, bin, sys, or system | 0600 |
| Management Information Base (MIB) files | | | 0640 |
| /etc/syslog.conf file | root | root, bin, sys, or system | 0640 |
| SSH public host key files | | | 0644 |
| SSH private host key files | | | 0600 |
| | | | |

### SEC-CRE-ROOT - Maintain careful control over root account

OS MUST by default secure the root account. The following requirements MUST be met:

- root account MUST be the only account having a UID of 0.
- root account's executable search path MUST be the vendor default and must contain only absolute paths.
- root account's library search path MUST be the system default and must contain only absolute paths.
- root account's list of preloaded libraries MUST be empty.
- root account MUST not have world-writable directories in its executable search path.
- system MUST prevent the root account from directly logging in except from the system console.
- system MUST not permit root logins using remote access programs such as ssh.

### SEC-DEF-SVC – Disable unnecessary service to reduce attack surface

OS MUST disable following services or not install them by default (mainly drawn from STIG UNIX version 1.0):

- portmap or rpcbind
- rsh/rshd
- rlogind

- rexec/rexecd
- telnet
- File Service Protocol (FSP)
- UUCP service active.
- Stream Control Transmission Protocol (SCTP)
- Datagram Congestion Control Protocol (DCCP)
- Lightweight User Datagram Protocol (UDP-Lite)
- Internetwork Packet Exchange (IPX) protocol
- AppleTalk protocol
- DECnet protocol
- Reliable Datagram Sockets (RDS) protocol
- Transparent Inter-Process Communication (TIPC) protocol
- Proxy Neighbor Discovery Protocol (NDP)
- DHCP client

# 6 Credentials

### SEC-LOG-INDC - Indicate password status at login

The following indications SHOULD be provided upon successful login as part of interactive user interfaces:

- That a password just used for authentication is about to expire, if this is true. The interval during which this information is displayed MUST be administratively configurable over a range at least from 0 to 30 days, and MUST default to 15 days. The indication MUST give the actual time remaining before password expiry.
- The last time at which a user ID was successfully used for authentication, the name of the authenticating host, the name or address of the location from which the user last received service, and the type of service used.
- The number of failed login attempts since the last successful login, together with the information normally given for a successful attempt.

### SEC-BAN-BEFR-2 - Ability to display configurable banner before login

It SHOULD be possible to administratively configure banner text to be displayed to users before authentication is requested. At least 1600 characters of text SHOULD be supported. The administrator SHOULD be able to enforce user acceptance of the text displayed on the click through banner before being allowed to navigate to the login page.

### SEC-BAN-AFTR-2 – Ability to display configurable banner after login

It SHOULD be possible to administratively configure banner text to be displayed to users immediately after authentication is completed. At least 1600 characters of text SHOULD be supported. This includes desktop login and FTPS/FTP login.

### SEC-INC-USER - Do not disclose username validity on failed login

When an invalid username/CREDENTIAL combination is presented, the response to the user or device attempting to log in MUST be only that the authentication has failed. Information regarding the validity of the username itself MUST NOT be provided.

### SEC-NUM-SESS-2 - Limit the number of concurrent sessions for one user

It SHOULD be possible to restrict each user to no more than a set number of sessions. This limit SHOULD be configurable on a per-user basis in the range from 1 through either 100 or the largest number of user sessions the OS is capable of supporting, whichever is less. It SHOULD be possible to disable the limit on a per-user basis.

### SEC-IDL-TMOUT-2 - Enforce idle session timeout

It MUST be possible either to configure a system wide timeout after which idle sessions will automatically be terminated, and/or to configure such timeouts on per-user or per-group basis, or at other granularities. It MUST be possible to ensure that some timeout is applied to every possible user.

### SEC-DEF-CRED-2 - No weak INBOUND CREDENTIALs except in CLEAN STATES

Except for CREDENTIALs used only for installation of OS, all INBOUND CREDENTIALs MUST be:

1. Generated by users or other entities outside of and not under the control of the OS, without prompting or specific suggestions from the OFFERING,
   OR
2. Generated at random by the OS itself, at or after installation time, using cryptographic-grade PRNGs which make the results unpredictable to any party, including Cisco, and disclosed by the OFFERING only to or as explicitly directed by the user, ADMINISTRATOR, or ADMINISTRATION device which commanded the creation of the CREDENTIAL in question.

### SEC-INT-CRED-2 - Disable weak installation CREDENTIALs after install

A new or “cleaned” OS MAY accept default or predictable credentials for installation, and MAY enable an administration protocol by default at installation time, provided that the software MUST force both to be disabled before regular operation begins.

### SEC-NRCV-CRED-4 - Hash non-recoverable stored CREDENTIALs

The system MUST use a FIPS 140-2 validated cryptographic module (operating in FIPS mode) for generating system password hashes. Passwords MUST be stored as hashes when there's no need to know the cleartext of the passwords. The use of SHA-256 or SHA-384 instead of SHA-1 is RECOMMENDED, Salts with at least 64 bits of entropy are also RECOMMENDED.

### SEC-USR-FAIL – Handle failed login appropriately

OS MUST provide capability to limit the number of failed logins, and disable account after that limit has been reached. Additionally, a delay between failed login prompts SHOULD be configurable.

### SEC-USR-MESS - Log only valid usernames for failed login attempts

When generating an audit message for a failed login attempt caused by an incorrect username/password pair:

- If the username given is a valid one, then the username MUST be included in the audit message.
- If the username given is *not* a valid one, then the username MUST NOT be included in the audit message (due to common mistake of user accidentally typing in password into the user name field).

### SEC-PWD-AUDIT - Never log passwords

Passwords MUST be excluded from all audit records, including records of successful or failed authentication attempts.

### SEC-RES-LOSS-2 - Recover from loss of authentication credentials

OS MUST provide a means for the ADMINISTRATOR to recover control of the OS when all ADMINISTRATOR CREDENTIALs have been lost. This method MUST be publically documented so that the recovery mechanism does not constitute a backdoor (SEC-CRE-NOBACK).

### SEC-ERA-DATA-2 - Support credential loss recovery via CLEAN STATE

OS MUST support a configuration wherein the use of the lost credential recovery mechanism will restore the system to a CLEAN STATE. Other lost credential recovery behaviors, including less drastic levels of configuration erasure, MAY additionally be supported when configured by the ADMINISTRATOR.

### SEC-CRE-REST-2 - Enforce password complexity

OS MUST be capable of enforcing the following restrictions:

- That the new PASSWORD contain characters from at least three of the following classes: lower case letters, upper case letters, digits, and special characters.
- That no character in the new PASSWORD be repeated more than three times consecutively.
- That the new PASSWORD not be the same as the associated username, and not be the username reversed.
- PASSWORD length restrictions (min and max).

It MUST be possible to individually enable or disable each of these restrictions as part of the configuration. A user interface MAY be provided for one-time overriding of the restrictions when a password is being set by an ADMINISTRATOR.

### SEC-SUP-CHAR-2 - Support all struck ASCII characters in passwords

Any struck character from the ASCII character set MUST be supported in passwords. A "struck" character is a character that would cause the printhead of a printing terminal to strike the paper; in other words, they are the characters that are associated with visible glyphs.

The struck ASCII characters are as follows:

```
!"#$%&'()*+,-./

0123456789

:;<=>?@

ABCDEFGHIJKLMNOPQRSTUVWXYZ

[\]^_`

abcdefghijklmnopqrstuvwxyz

{|}~
```

### SEC-MIN-INTV - Ability to enforce minimum end-user password change interval

It SHOULD be possible to administratively restrict the number of password changes an end user can make within a given time.

### SEC-PWD-REUSE - Restrict end-user password reuse

At any end-user password change, the new password SHOULD, by default, be rejected if it is the same as any previously used password for the same user, up to an administratively configurable history depth which SHOULD default to 5, and which SHOULD support configuration up to 15.

### SEC-CHG-INTV - Enforce maximum end-user password lifetime

It SHOULD be possible to administratively specify that passwords which have not been changed within a configurable interval are to be automatically disabled.

### SEC-PWD-CHECK - Restrict passwords only at password change

OS checking passwords at user authentication time MUST ignore password complexity constraints. Only entities controlling password changes are to apply such constraints.

### SEC-CHG-PSWD-2 - Authenticate at password changes

When a user changes his or her own PASSWORD using a user interface designed for this purpose, authentication using the old password MUST, by default, be required immediately before the new password is set. It is acceptable to permit administrative change to this behavior.

## 7 Protocol

### SEC-OFF-PROC - Selectively enable TCP/IP SERVICEs (incl. OPEN PORTs)

It MUST be possible for an ADMINISTRATOR to separately enable or disable each provided TCP/IP SERVICE, except that any set of TCP/IP SERVICES which are MUTUALLY ESSENTIAL MAY be configured as a group.

### SEC-WEL-PORT-2 - Don't run the wrong protocols on well-known ports

By default, OS SHOULD NOT direct incoming traffic on TCP or UDP ports numbered from 1 to 1024 to LISTENERs implementing protocols other than those for which those ports are registered with IANA/CANA.

For example, TCP port 80 SHOULD NOT be used for other than HTTP, and TCP and UDP ports 53 SHOULD NOT be used for other than DNS.

Ports outside the range from 1 to 1024 SHOULD be evaluated according to their common usages in each OFFERING's usual environment; for example, it rarely makes sense to use port 2049 for other than NFS.

### SEC-CON-PERM - Filter incoming connections by source IP address

OS MUST be capable of limiting connections to any service on the OS based on source IP address(es) of the connecting entities.

*Application Note: On Linux, the kernel should include netfilter/iptables, and the distribution should include userspace 'iptables' package.*

### SEC-LIM-TRAF - Configurably rate-limit IP based on layers 3 and 4

OS MUST provide ADMINISTRATOR configurable rate limiting for TCP, UDP, IP and ICMP traffic directed to or through the device. It MUST be possible to rate limit traffic based on the values of any field or combination of fields in the outermost IP header. When the transport protocol is TCP or UDP, it MUST further be possible to rate limit traffic based on any field or combination of fields in the TCP or UDP header.

### SEC-TCP-RAND - Randomize initial TCP sequence numbers

Initial TCP sequence numbers MUST be selected in a way unpredictable to remote attackers. A cryptographic-grade pseudorandom number generator SHOULD be used for this purpose.

### SEC-ARP-STAT-2 - Support static IP-to-MAC address bindings

OS SHOULD support ADMINISTRATOR configuration of static bindings between IP addresses and link-layer addresses. These entries SHOULD be protected from overwriting by dynamic data received from the network.

### SEC-SSH-V2.0 - Support SSH v2

OS MUST support SSH version 2, which is Cisco's and the Internet's de facto standard protocol for interactive logins. Telnet and SSH version 1 are obsolete. The SSH daemon and client must use a FIPS 140-2 validated cryptographic module (operating in FIPS mode).

- The SSH daemon and client must be configured to not use CBC ciphers (vulnerable to chosen-plaintext attacks).
- The SSH daemon must perform strict mode checking of home directory configuration files.
- The SSH daemon must use privilege separation.
- The SSH daemon must not allow rhosts RSA authentication.
- The SSH daemon must not allow compression or must only allow compression after successful authentication.
- The SSH daemon must be configured for IP filtering.

### SEC-DHCP-RAND - Randomize DHCP Transaction ID fields

MANDATORY for all DHCP clients using DHCP attributes other than IP address and netmask with the following attributes:

- The transaction ID, or “xid” field in each generated DHCP request SHALL be generated in such a way as to be unpredictable by any remote attacker. A DHCP

client SHALL NOT use the same sequence of “xid”s at each restart, and each request's “xid” field SHALL be independent of the “xid” field in any other request.
- DHCP responses with incorrect “xid” fields MUST NOT be processed.
- “xid”s SHOULD be generated using a cryptographic-grade pseudorandom number generator.

### SEC-TIME-NTP - Use NTP for date and time maintenance

OS MUST support obtaining date and time information using the Network Time Protocol, NTP version 3 as specified in RFC 1305, including the authentication options. It is RECOMMENDED that the OS track and support NTP version 4, which has had a relatively stable reference implementation for some time.

### SEC-NTP-IPFILT - Separately filter NTP peers and clients by IP address

It MUST be possible to specify separate IP address filters listing hosts which MAY be considered as time sources and hosts which MAY synchronize with the local host as NTP clients.

### SEC-NTP-AUTH3 - Support NTPv3 authentication

Each NTP implementation MUST support symmetric-key authentication in the style of NTP version 3, as defined in RFC 1305, in both client and server roles.

### SEC-NTP-AUTH4 - Support NTPv4 authentication

Each NTP version 4 implementation MUST support NTP version 4 public key authentication.

### SEC-SNM-AES - Support AES-128 for SNMPv3

All SNMP implementations MUST support SNMPv3 encryption using AES with at least a 128-bit key. The SNMP service SHOULD use a FIPS 140-2 approved cryptographic hash algorithm as part of its authentication and integrity methods.

### SEC-SNM-SHA96 - HMAC-SHA-96 for SNMPv3 authentication

All SNMP implementations MUST support SNMPv3 authentication using HMAC-SHA-96. The SNMP service SHOULD use a FIPS 140-2 approved cryptographic hash algorithm as part of its authentication and integrity methods.

### SEC-HTP-SSL3-2 - Support TLS and negotiate SSLv3 for HTTP

Any HTTP server or client MUST be capable of being configured to provide TLS encryption for all HTTP traffic, and MUST furthermore be capable of negotiating down to SSLv3. Clients MUST have the capability to supply their own TLS package in place of the system default one.

### SEC-IPS-ESP-3 - Support IPsec ESP encryption for all unicast IP

Each IP implementation MUST support IPsec ESP for all locally originated or terminated unicast IP traffic. This MUST extend to implementation of IKE for keying.

*Application Note: This capability is fully supported on native IPsec stack in Linux kernel 2.6.*.*

### SEC-IP-IPv6 - Support all security requirements over IPv6

Every function and protocol required for IPv4 is also required for IPv6, except for requirements which explicitly say they address only IPv4 or and requirements concerned with elements of IPv4 which do not exist in IPv6, *every* requirement in this document applies to IPv6 (and TCPv6, UDPv6, ICMPv6, DHCPv6, etc) as well as to IPv4.

As particular examples of this very general rule:

- Required protocols (NTP, SYSLOG, SSH, IPsec, etc) MUST be implemented over IPv6 as well as over IPv4, and all required functionality.
- Filtering, logging, and robustness requirements apply to IPv6 as well as to IPv4
- Requirements on the implementation of various protocols apply to the IPv6 versions of those protocols as well as to the IPv4 versions.

### SEC-IPv6-LMT – Ability to set upper bound on IPv6 prefix list and reconfiguration

The IPv6 implementation MUST be able to set an upper bound on the number of prefixes being added to the device prefix list and number of addresses automatically configured due to router advertisements.

### SEC-IPv6-SeND – Implement IPv6 Secure Neighbor Discovery Protocol (SeND)

The IPv6 implementation SHOULD implement SeND protocol defined in RFC 3971.

### SEC-IPv6-CGA – Implement IPv6 Cryptographically Generated Address

The IPv6 implementation SHOULD implement the ability to form Cryptographically Generated Address as defined in RFC 3972.

### SEC-IPv6-USGv6 – IPv6 implementation MUST be USGv6 compliant

The IPv6 implementation MUST be compliant with "A Profile for IPv6 in the US Government – version 1.0".

### SEC-DNS-DNSSEC - Fully support DNSSEC for all DNS applications

OS MUST support DNSSEC, in accordance with the document references of this requirement.

RFC 4033, DNS Security Introduction and Requirements.
RFC 4034, Resource Records for the DNS Security Extensions.
RFC 4035, Protocol Modifications for the DNS Security Extensions.

RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
RFC 5074, DNSSEC Lookaside Validation (DLV).
RFC 4431, The DNSSEC Lookaside Validation (DLV) DNS Resource Record.

RFC 3225, Indicating Resolver Support of DNSSEC. (updated by RFC4035)

RFC 2671, Extension Mechanisms for DNS (EDNS0).
RFC 3226, DNSSEC and IPv6 A6 aware server/resolver message size requirements.
RFC 3597, Handling of Unknown DNS Resource Record (RR) Types.
RFC 5625, DNS Proxy Implementation Guidelines.

RFC 4641, DNSSEC Operational Practices.
RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors.
RFC 4986, Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover
draft-icann-dnssec-arch-v1dot4.pdf, DNSSEC Root Zone High Level Technical Architecture.

RFC 3007, Secure Domain Name System (DNS) Dynamic Update.
RFC 2136, Dynamic Updates in the Domain Name System (DNS UPDATE).
RFC 2845, Secret Key Transaction Authentication for DNS (TSIG).
RFC 3645, Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG).
RFC 2930, Secret Key Establishment for DNS (TKEY RR).

http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml
RFC 5933, Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC.
RFC 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC.
RFC 4635, HMAC SHA TSIG Algorithm Identifiers.
RFC 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs).
RFC 3110, RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS).

*Application Note: On Linux, the most widely used code for local validating resolver is "unbound" (http://www.unbound.net). Unbound can be used as a library linked with a C application (in place of the standard libc functions), or run as a local server (remember to make sure only the local machine can talk to it). Either configuration can be made fully compliant with this requirement.*

# 8 Crypto

Note requirements for user land ssl package have been intentionally left out of this document. Vendors may simply provide latest openSSL package available at the time of building the distro.

### SEC-KER-FIPS – Kernel Crypto Module must be FIPS 140-2 certified

OS kernel crypto module must be FIPS 140-2 certified. The specific algorithms expect to be provided by the kernel include, but is not limited to:

- IPSec
  - AES-CBC, AES-GCM with all key sizes
  - SHA-1
  - HMAC-SHA1
  - HMAC-SHA-256
- Disk Encryption
  - AES-XTS with all key sizes

# 9 Toolchain and Process

### SEC-RUN-OSC - Provide support for Object Size Checking (BOSC)

The C/C++ compiler MUST support OSC functionality, which is a compiler technique that identifies buffer overruns. It causes the compilation to fail when compiler can determine at compile time that certain function calls are potential overflows. The compiler also remaps eligible buffer-manipulation function calls to more tightly-bounded versions to help prevent overflows at run time.

The following high risk functions MUST be supported by the compiler

| Destination Bounded | Source Bounded | Unbounded |
|---|---|---|
| strncpy<br>strncat | memcpy<br>bcopy | strcpy<br>strcat |

| | | |
|---|---|---|
| snprintf | bzero<br>memmove<br>memset | sprintf |

*Application Note: GCC 4.5+ provides this functionality. Although earlier versions of GCC do implement this functionality, GCC 4.5+ is the minimum version with enough feature support to meet Cisco's requirements.*

### SEC-RUN-PROP - Provide support for Stack Smashing Protection

The C/C++ compiler MUST provide Stack Smashing protection. Typically, this is done through the use of a canary inserted onto the stack just prior to the function return address to detect buffer overwrite.

*Application Note: GCC 4.5+ provides this functionality.*

### SEC-RUN-SA - Run Static Analysis and fix high priority security defects

The vendor MUST run static analysis tool to detect security defects in the source code, and fix high priority issues found. The list of high priority issues include but not limited to:

| | |
|---|---|
| Tainted Input | Use of input from client without validation. This could lead to injection attacks such as command injection. |
| Buffer Overflow | Incorrect usage of buffer copy functions such as strcpy() and memcpy() by copying a source buffer that is too large to fit into the destination buffer. |
| Null Pointer Deference | Attempt to dereference a pointer that had been set to null |
| Access Memory After Free | Attempt to dereference memory after it has been freed |
| Invalid Array or Pointer Arithmetic | Attempt to increment/decrement array index or pointers pass bounds of an array |
| Resource Leaks | Possible resource leaks due to unclosed system resources such as file, socket, database connections |

### SEC-SUP-SFT – Provide inventory of all user space code

The vendor MUST provide an inventory of all 3rd party code and the associated versions which are included in the distro.

### SEC-SUP-SRC – Provide source code for toolchain

The vendor MUST provide source code and change log to the toolchain that is part of the distro. This allows Cisco to perform security audits on the toolchain if needed, as well as regenerate the toolchain in the future.

### SEC-SUP-PATCH - Security Incident notification and response

The vendor MUST notify Cisco of security incidences (CVE) against code/packages that is part of the OS distribution in a timely manner (agreed upon at the time of the contract negotiation). Security patches for these code/packages MUST be incorporated, validated, and shipped to Cisco in a timely manner. The patches must be delivered in the following format:

- Patched version of Linux distro made available to Cisco (previous versions delivered to Cisco and the latest)
- Standalone patch for Cisco engineering, as it is not always practical for Cisco to upgrade to later version of kernel.
- Document CVEs addressed in the patch. If certain CVEs are not addressed, the vendor MUST document the reason.

### SEC-CERT-STIGS – Receive UNIX or RED HAT STIGS certification

OS SHOULD go through "UNIX General" or "Red Hat 5" STIGs certification.

### SEC-CERT-CC – Receive Common Criteria certification

OS SHOULD receive Common Criteria Certification at Enterprise Assurance Level 4 (EAL4+) under the Operating System Protection Profile (OSPP).

## 10 Future Requirements

This section describes some possible future security requirements for Linux distribution vendors. They are not listed in the main requirements sections primarily due to issues such as lack of proven implementations or potential performance and memory impact.

### Randomize Linux Kernel base address

The ASLR requirements in this document mainly covered process address spaces. The base address of the kernel (address at which the kernel is decompressed by the bootloader) should be randomized to mitigate exploit attempts replying on the location of kernel internals.

### Linux Loadable Kernel module signing and verification

Linux loadable kernel modules provide a way to extend the kernel at runtime. Typical examples of LKMs include device/filesystem/network drivers and system calls. The actual content of the module or security risks at the time of loading is a not known to the kernel. Given that a loadable kernel module runs with full kernel privilege, it is important for the system to have the capability to validate a "trusted" or signed kernel module through verification of its digital signature.