Hardening Guidelines

This appendix contains the following section:

Hardening Guidelines

If you consider hardening the system, you should consider the following hardening guidelines:

- Refer to the host platform's hardening guides. For example:
  - RHEL/CentOS 7.x:

    https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Security_Guide/Red_Hat_Enterprise_Linux-7-Security_Guide-en-US.pdf
  - RHEL/CentOS 8.x:

    https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/security_hardening/Red_Hat_Enterprise_Linux-8-Security_hardening-en-US.pdf

    https://www.cisecurity.org/benchmark/red_hat_linux/

    https://www.cisecurity.org/benchmark/centos_linux/
  - NSA hardening guide collection:

    https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

Note The above links reference external websites and Cisco is not responsible for keeping them up-to-date. They are provided for reference only. If you find that the content is outdated or if you cannot access the links, please contact the website owner for updated information.

- Disable or block the ports that are not used by Cisco Prime Network Registrar. The Cisco Prime Network Registrar documentation outlines the port usage and also the issues with using firewall items, such as connection tracking.

- For a list of ports used by Cisco Prime Network Registrar, see the *"Default Ports for Cisco Prime Network Registrar Services" section in the Cisco Prime Network Registrar 11.0 Administration Guide*. Note that some are defaults and may have been changed during install or configuration.
- For connection tracking related issues, see the *"DNS Performance and Firewall Connection Tracking" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

- Install Cisco Prime Network Registrar using the non-root account and use the security features (that is, https and require secure SCP sessions).
- Confirm that any product directories (primarily, /opt/nwreg2/* and /var/nwreg2/*) are locked down as appropriate. Note that you may need to adjust the protection based on your needs (such as for performing offline backups and viewing logs).
- DNS specific considerations include:
  - Use DNS Security Extensions (DNSSEC):

    DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks. DNSSEC provides protection against malicious or forged answers by adding digital signatures into DNS data, so each DNS response can be verified for integrity and authenticity.

    Cisco Prime Network Registrar 9.0 and earlier Authoritative DNS Server do not support signing of zones. Starting from Cisco Prime Network Registrar 10.0, Authoritative DNSSEC support adds authentication and integrity to DNS zones. With this support, Cisco Prime Network Registrar DNS server is able to support both secure and unsecure zones. For more information, see the *"Managing Authoritative DNSSEC" section in the Cisco Prime Network Registrar 11.0 Authoritative and Caching DNS User Guide*.
  - Secure DNS server activity with ACLs:
    - Restricting Zone Queries—The *restrict-query-acl* attribute on the DNS server serves as a default value for zones that do not have *restrict-query-acl* explicitly set.
    - Restricting Zone Transfer Requests—Use the *restrict-xfer-acl* attribute to filter the zone transfer request to the known secondary servers.
    - Restricting DDNS Updates—Use the *update-acl* attribute to filter DDNS packet from the known DHCP servers.
  - Secure zone transfers and DNS updates using TSIG or GSS-TSIG:

    Zone transfer in secure mode supports both HMAC-MD5 based TSIG and GSS-TSIG. You can add an optional TSIG key or GSS-TSIG keys (see the *"Transaction Security" or "GSS-TSIG " sections in the Cisco Prime Network Registrar 11.0 DHCP User Guide*) to the primary server address by hyphenating the entry in the format *address–key*. For each entry, click **Add IP Key**.

    For more information, see the *"Creating a Zone Distribution" section in the Cisco Prime Network Registrar 11.0 Authoritative and Caching DNS User Guide*
  - Randomize Query IDs and Source Ports.
  - DNS Rate Limiting—See the *"Managing Caching Rate Limiting" section in the Cisco Prime Network Registrar 11.0 Authoritative and Caching DNS User Guide*.
  - Separate Recursive Server and Authoritative Server roles.

- DHCP specific considerations include:
  - Assure DHCPv4 and DHCPv6 traffic from the "external" sources is blocked on routers and that only valid relay agents are enabled to forward packets to the DHCP servers.
  - Use DHCP Guard and similar services on switches:

    See https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcpsnoop.html

    See https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/ip6-dhcpv6-guard.pdf
  - Use the Chatty Client Filter—See the *"Preventing Chatty Clients by Using an Extension" section in the Cisco Prime Network Registrar 11.0 DHCP User Guide*.
- Consider using external user authentication as password rules (that is, change frequency, length, and difficulty checks) can typically be implemented for Active Directory (LDAP) and RADIUS users. See the *"External Authentication Servers" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

Hardening Guidelines