Understanding DNSSEC

Fedora Change

PRESENTED BY:

Tomas Hozza

Red Hat

Today's Topics

- Why is DNSSEC important
- What is the change about
- How it works
- Integration in Fedora products
  - Workstation, Server, Cloud, Other variants

Why is DNSSEC important

DNS and DNSSEC

- DNS - distributed database for various data
- Trusted data
  - TLSA, SSHFP, IPSECKEY, CERT, CAA
  - Possibilities for new kinds of applications
- Plain DNS - vulnerable
- DNS SECurity extensions
  - Provide data authenticity and integrity
  - Chain of trust from the “.” root zone
-

What is the change about

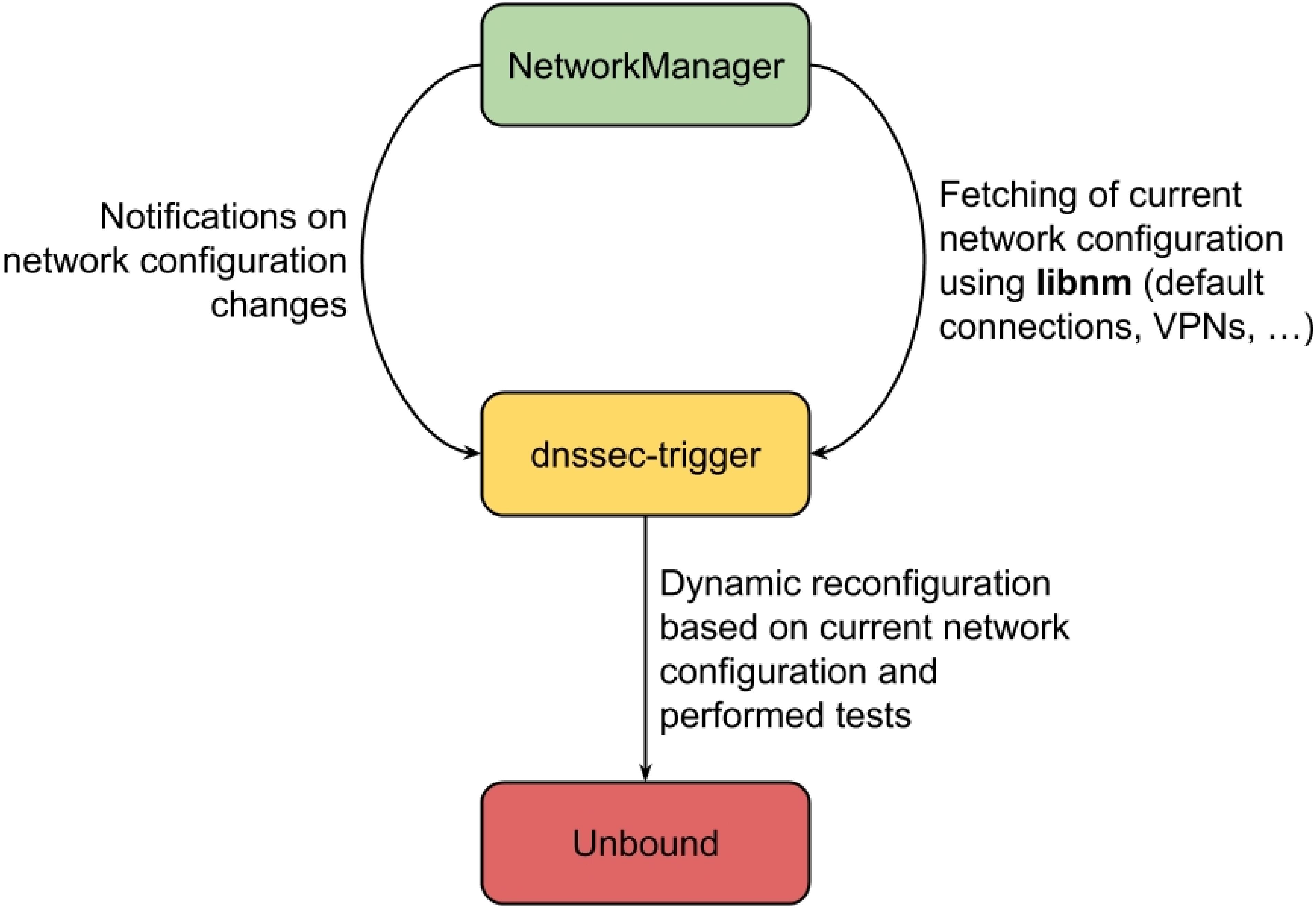
Integration

- Focus on (application) client side
- Integration of multiple components into one solution
- Responding to network configuration changes
- Local validating resolver - increase DNS security also for applications that “don’t care”
- Applications that do care will use some validating DNS API

How it works in Fedora

Details

- NetworkManager
  - Network configuration manager
- Unbound server
  - Validating DNS resolver
- dnssec-trigger
  - Integration component between Unbound and NM
  - Handling of network configuration changes



NetworkManager
Notifications on network configuration changes
Fetching of current network configuration using **libnm** (default connections, VPNs, …)
dnssec-trigger
Dynamic reconfiguration based on current network configuration and performed tests
Unbound

Supported functionality

- VPNs and “Split DNS” view
- Private IP network ranges
- Fallback mechanisms
  - Full recursion
  - DNS over TCP (port 80)
  - DNS over SSL (port 443)

Integration in Fedora products

Fedora products

- Each product has specific audience
- Product specific configuration
- Integration points
  - Captive portal detection
  - Captive portal login handling
  - User interaction

Common things

- dnssec-trigger panel not installed by default
- Captive portal detection turned off
  - will rely on NetworkManager
  - Connection state change notifications from NM are still pending

Fedora Workstation

- Captive portal login left completely up to GNOME Shell
- No user interaction (but can be changed)
- Automatic switch to INSECURE mode if all fallback options failed

Cloud (Host)

- Have trusted resolver on the (Atomic) Host
- Containers reusing the local (to host) resolver
- No local resolver on cloud Images
- Docker
  - can not use “127.0.0.1” in resolv.conf
  - iptables and DNAT “hack”
  - https://github.com/docker/docker/issues/14627

Server

- configuration
  - manual
  - automatic using dnssec-trigger
- dnssec-trigger-control
  - substitutes the dnssec-trigger panel in CLI

Other variants

- need to install dnssec-trigger panel for UI
- rest is the same as for others Products

Summary

- DNSSEC on client side opens new possibilities
- Tightly integrated set of components
- Different configuration for different products
- Some “dirty hacks” commonly used with plain DNS will stop working
- Please test it for your use-cases

Links

- https://fedoraproject.org/wiki/Networking/NameResolution/DNSSEC
- https://fedoraproject.org/wiki/Networking/NameResolution/DNSSEC/Design
- https://fedoraproject.org/wiki/Networking/NameResolution/DNSSEC/UnboundMixedMode
- https://fedoraproject.org/wiki/Changes/Default_Local_DNS_Resolver

Questions?

CONTACT:
thozza@fedoraproject.org