DNSSEC on workstations

(But not only)

PRESENTED BY:

Tomáš Hozza
Petr Špaček

Today Topics

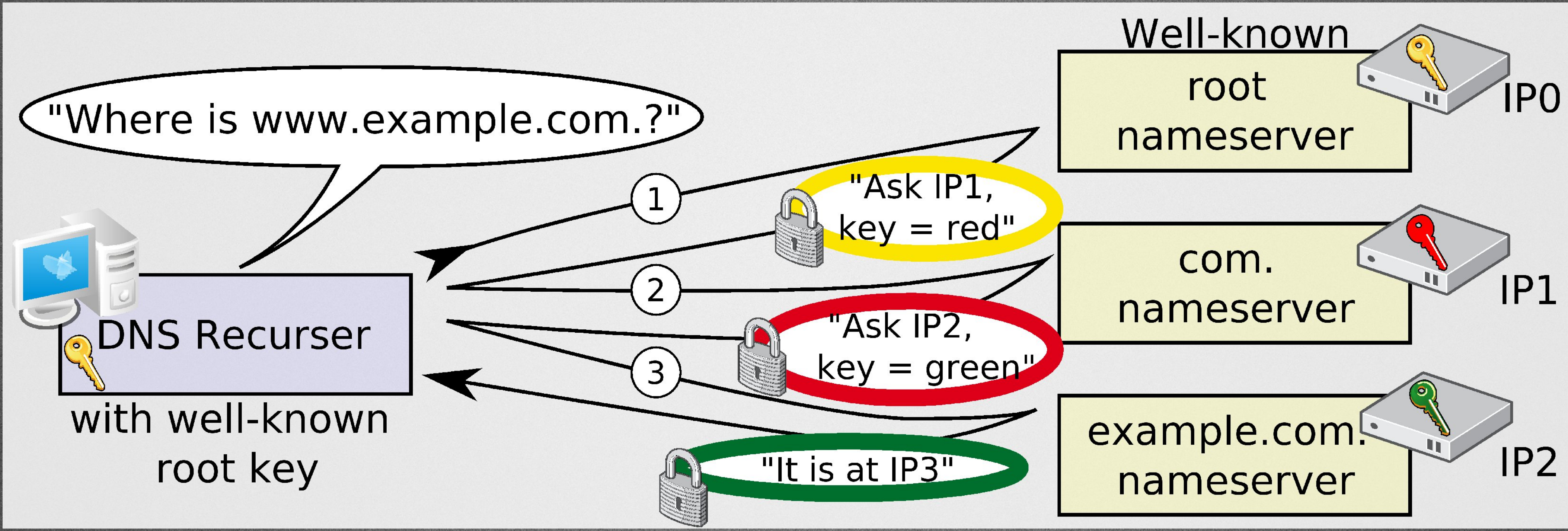
- DNSSEC in general
- Why is DNSSEC important?
- Client side
  - The current situation on client in Fedora
  - The (possible) future ahead
- Server side
  - FreeIPA

DNSSEC in general

Plain DNS vs. with DNSSEC

- Plain DNS is not secure
  - No response authenticity and integrity
  - Cache poisoning
- DNSSEC
  - Extension of plain DNS
  - Asymmetric cryptography
  - Guarantees the response authenticity and integrity

How DNSSEC works



Why is DNSSEC important?

Benefits

- You can trust the server's response
- Getting data from trusted source
  - Public keys (fingerprints)
  - Certificates
- DNSSEC enabled applications
  - SSH (SSHFP record - RFC 4255)
  - Certificates / Public keys (TLSA record - RFC 6698)
  - IPSec keys (IPSECKEY record - RFC 4025)

SSHFP records

- SSH public keys fingerprints verification

- The well known “leap of faith” question

```
$ ssh user@192.168.122.105
The authenticity of host ’192.168.122.105 (192.168.122.105)’ can’t be established.
RSA key fingerprint is 7e:1f:8c:19:4c:88:98:4e:54:09:9e:e2:df:3a:c7:40.
Are you sure you want to continue connecting (yes/no)?
```

- Openssh can verify the fingerprint for you

```
$ ssh -o “VerifyHostKeyDNS yes” user@192.168.122.105
```

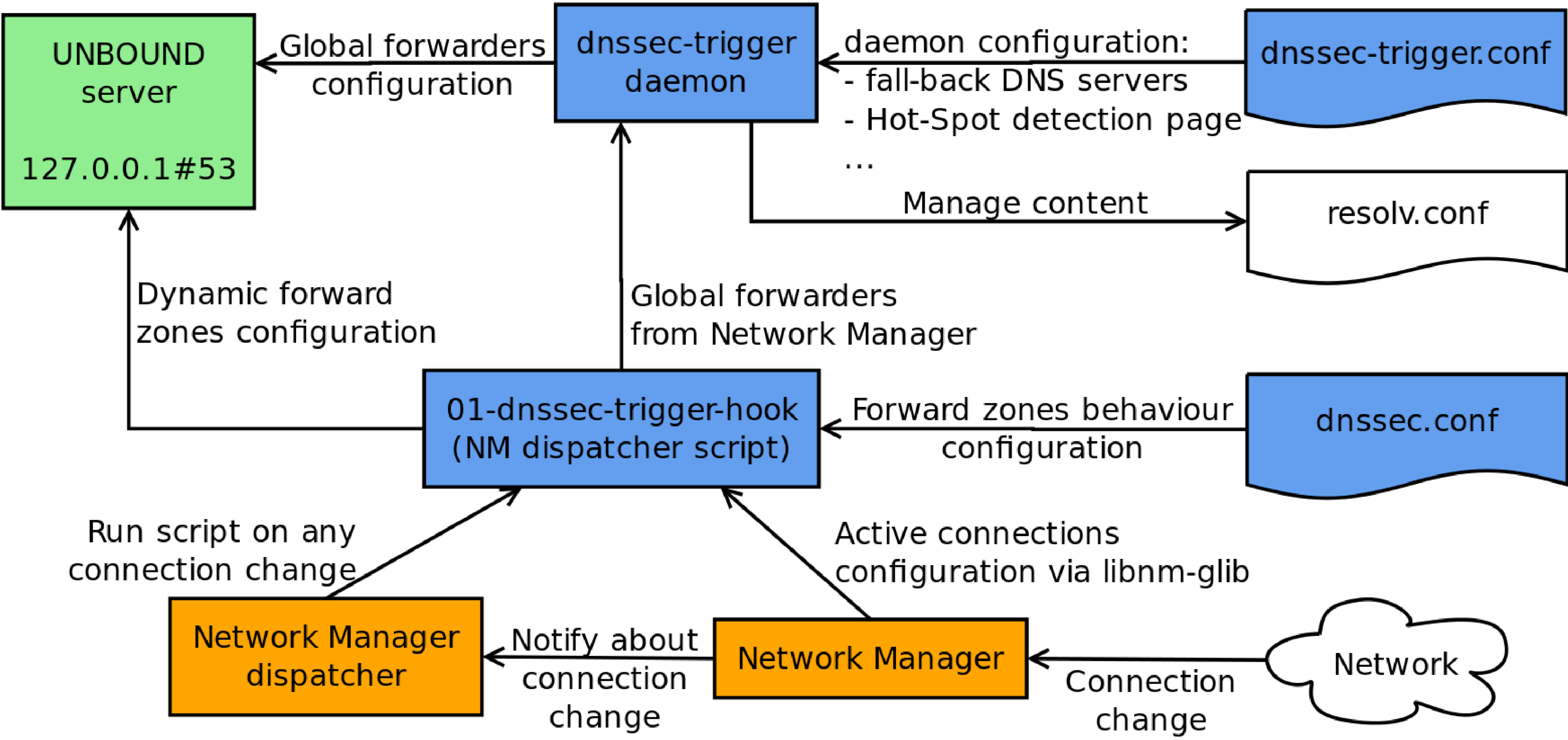
Client Side

Requirements

- Locally running validator
- Dynamic environment
  - Connections going up/down
- Need to handle connection provided domains
  - Split DNS configuration
- Some provided NS may be broken
  - Fall-back
- Hot-Spot detection

Situation in Fedora

- F17 Feature – DNSSEC on workstations
  - Functionality has been improved
- Validating resolver – unbound
- Reconfiguration daemon – dnssec-trigger
  - NM dispatcher script (using libnm-glib)
- Forward zones configuration
  - /etc/dnssec.conf


UNBOUND server
127.0.0.1#53
Global forwarders configuration
dnssec-trigger daemon
daemon configuration:
- fall-back DNS servers
- Hot-Spot detection page
...
dnssec-trigger.conf
Manage content
resolv.conf
Dynamic forward zones configuration
Global forwarders from Network Manager
01-dnssec-trigger-hook (NM dispatcher script)
Forward zones behaviour configuration
dnssec.conf
Run script on any connection change
Active connections configuration via libnm-glib
Network Manager dispatcher
Notify about connection change
Network Manager
Connection change
Network

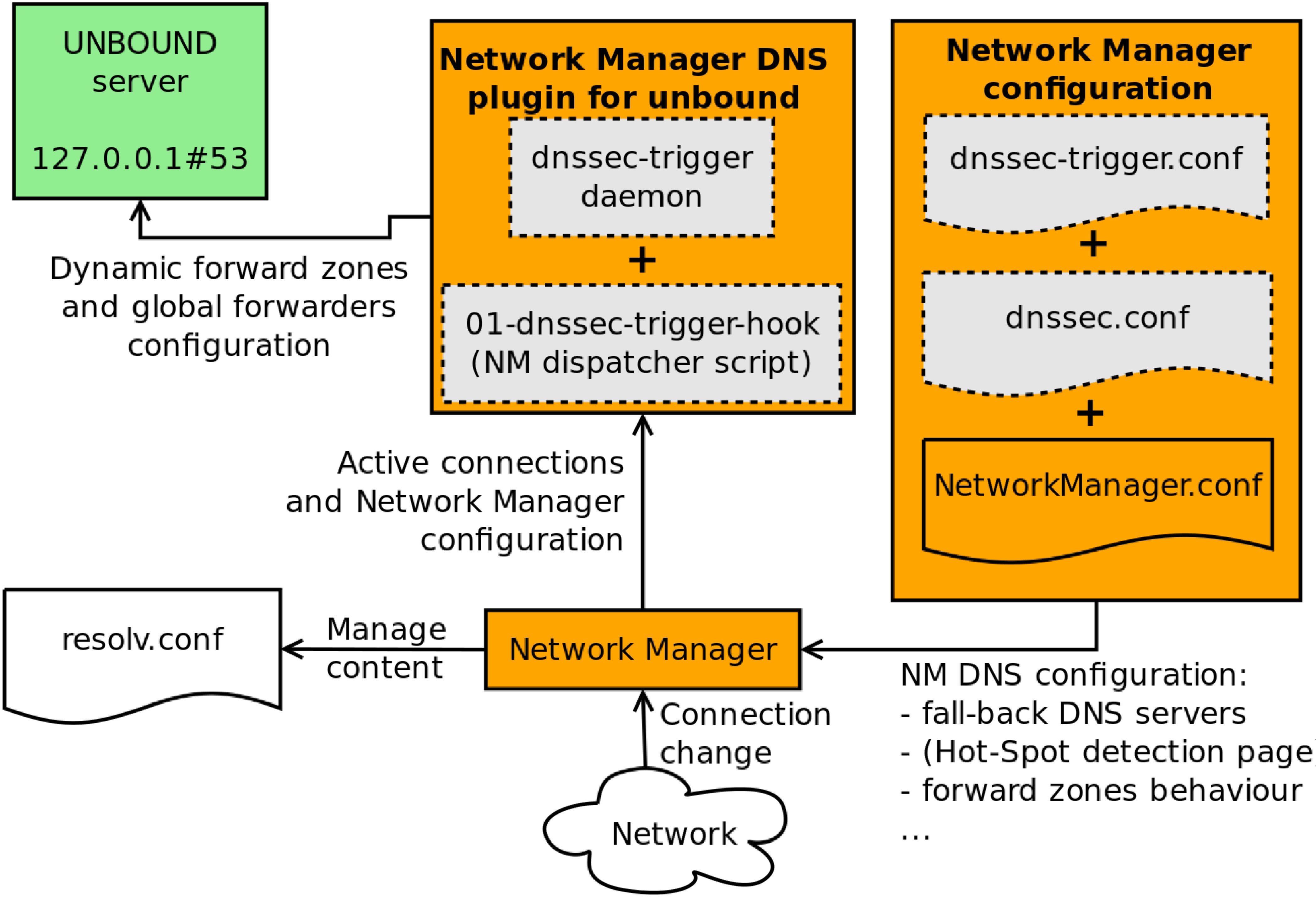
Known issues & Limitations

- Forward zones DNSSEC validation can be set only globally
- You may see some ABRT notifications
  - NM doesn't provide API to get Active Connection type
  - NM dispatcher does not serialize connection events
  - NM guys are working on these...

#DEFINE FUTURE

What is “the plan”

- Unbound DNS plug-in in Network Manager
- dnssec-trigger functionality implemented in Network Manager
    - Improved hot-spot detection
    - DNS servers probing for DNSSEC records
    - Fall-back configuration to DNSSEC capable servers
    - Per connection
        - Enable/disable DNSSEC
        - Enable/disable forward zones for provided domains


UNBOUND server
127.0.0.1#53
Network Manager DNS plugin for unbound
dnssec-trigger daemon
+
01-dnssec-trigger-hook (NM dispatcher script)
Network Manager configuration
dnssec-trigger.conf
+
dnssec.conf
+
NetworkManager.conf
Dynamic forward zones and global forwarders configuration
Active connections and Network Manager configuration
resolv.conf
Manage content
Network Manager
Connection change
Network
NM DNS configuration:
- fall-back DNS servers
- (Hot-Spot detection page
- forward zones behaviour
...

Server Side

FreeIPA?

- What is it?
- How is it related to DNSSEC?

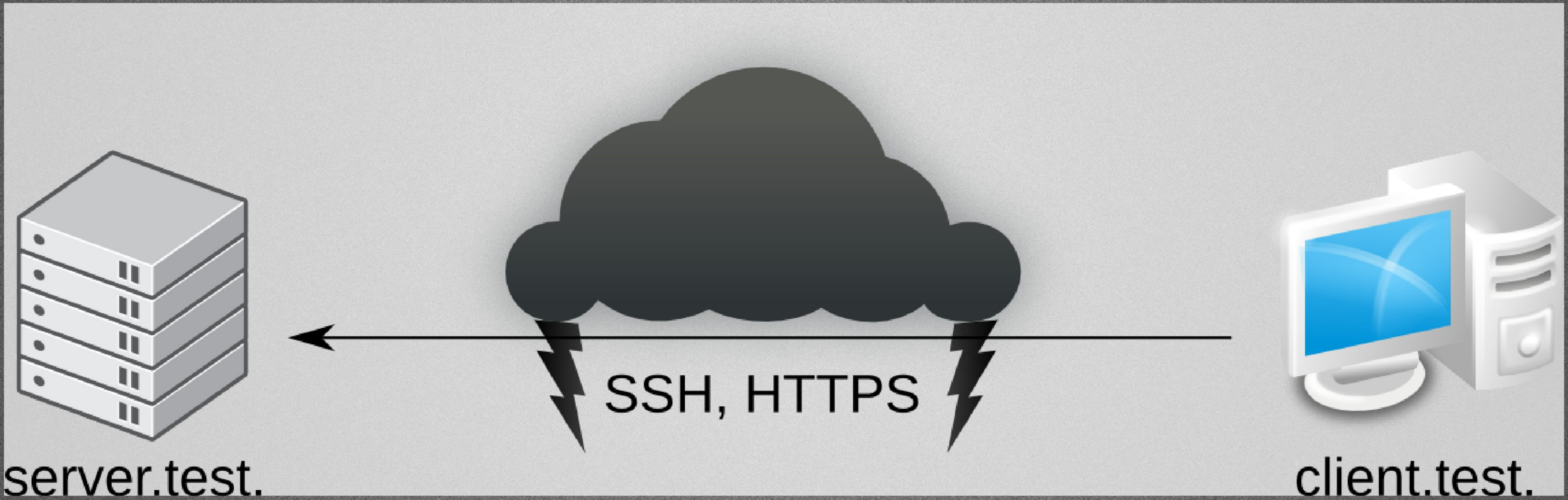
Free IPA !

SUPERFLEX
台灣啤酒
SUPERFLEX
TAIWAN
10 TB 台北雙年展
FREE BEER
TAIWAN
台灣自由啤酒

+

UNLIMITED RELEASE
LAGUNITAS
IPA
INDIA PALE ALE
Brewed and Bottled by the Lagunitas Brewing Co.
Petaluma, California.
O.G. 1.059
I.B.U. 45.6

How is identity management related to DNSSEC?



How can DNSSEC stop MitM attacks?

```
$ dig +dnssec -t TLSA _443._tcp.fedoraproject.org

;; ANSWER SECTION:

_443._tcp.fedoraproject.org. 300 IN   TLSA    0 0 1
D4C4C99819F3A5F2C6261C9444C62A8B263B39BC6ACCE35CD
CABE272 D5037FB2

_443._tcp.fedoraproject.org. 300 IN   RRSIG TLSA 5 4 300
20140308200942 20140206200942 7725 fedoraproject.org.
mjTMoPpFUQn5oGjOLFgQzYrgt6PNGJ/WcUHynW36j07S+6gPW
fP2LMknz+YkSZEJGy6SUNzVVetKMxhB27QSR6ePbcrTdi1DlxAh
9kL05Y8aTrKgixI7VyEyq9QkoWBVeS7fIkJh5hT2p5+ayCx3HzQt
OI7fTQ6eO0x3ubYM 5sE=
```

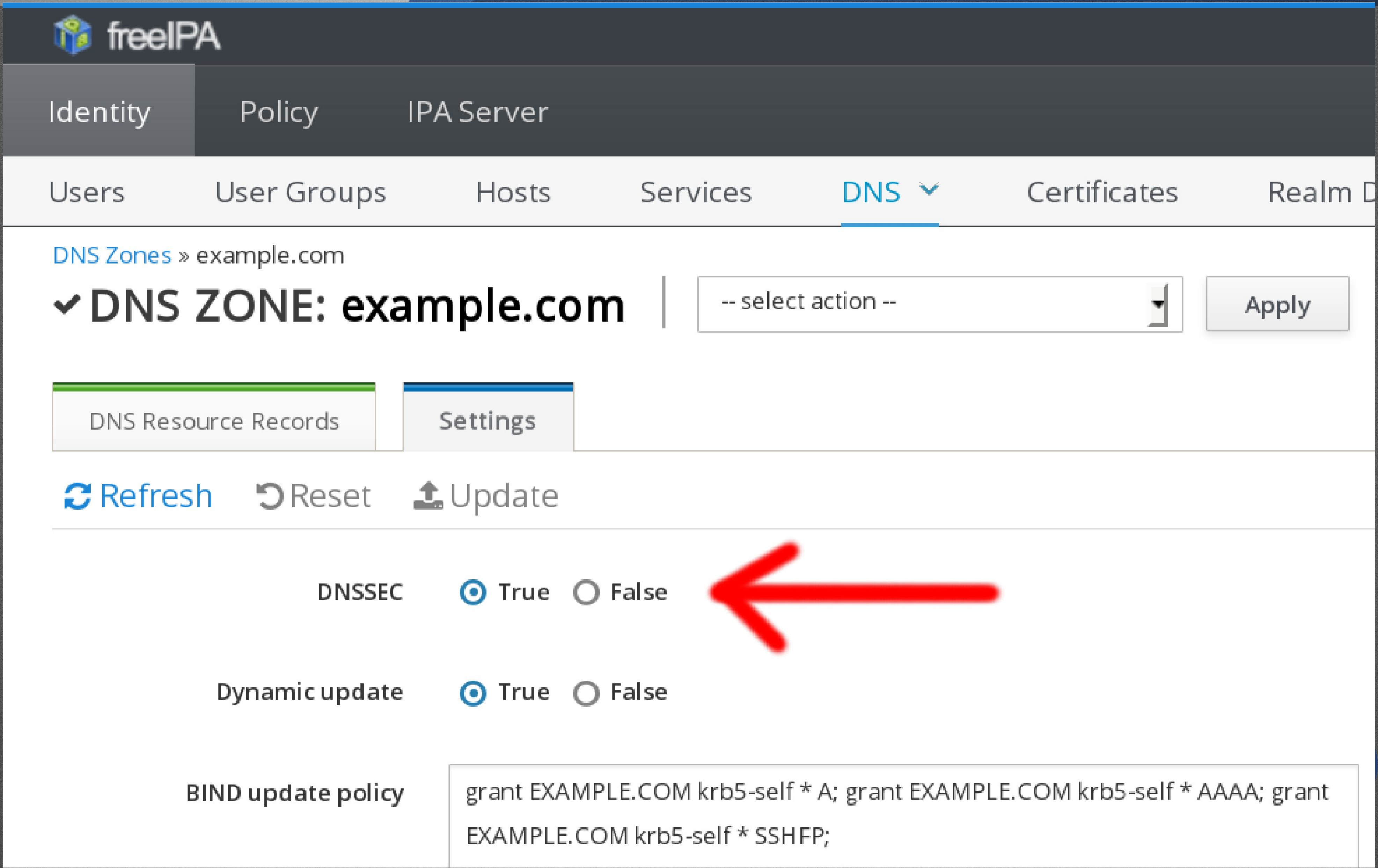
Why should you think about FreeIPA?

- You can do everything manually:
  - $ dnssec-keygen (two times)
  - $ dnssec-signzone
  - publish the key in parent DNS domain
  - rotate keys and re-sign all the data
    - repeat monthly!

- For each DNS zone separately

  OR ...

How can FreeIPA help you?



DNS Zones » example.com

✓ DNS ZONE: example.com

DNSSEC ● True ○ False

Dynamic update ● True ○ False

BIND update policy: grant EXAMPLE.COM krb5-self * A; grant EXAMPLE.COM krb5-self * AAAA; grant EXAMPLE.COM krb5-self * SSHFP;

FreeIPA #define future

- Automatic key rotation
  - look forward to Fedora 21
  - watch freeipa-interest@redhat.com list
- Client-side applications
  are waiting for your patches!
  - TLS certificates in DNS: RFC 6698
  - SSH public keys in DNS: RFC 4255
  - IPSec keys in DNS: RFC 4025
  - S/MIME keys in DNS: draft-ietf-dane-smime-04

Summary

- DNSSEC is important for security
  - Getting trusted data
  - Improves security also for DNSSEC-not-aware applications
- The client side implementation in OS is still work in progress and improving
  - We would love to hear users feedback

```
$ yum -y install dnssec-trigger
```

Feedback - http://devconf.cz/f/64

CONTACT:

thozza@redhat.com
pspacek@redhat.com