AGOSTO 2020

FORT
Paso a Paso

nic chile
SOMOS EL PUNTO CL

Celsa Sánchez, NIC Chile, .CL

CONTENIDO

Contenido

Fort Paso a Paso

RUTEO OPEN SOURCE

Open Source como complemento en nuestra infraestructura TI

Validador FORT

Validador RPKI
más
Servidor RTR

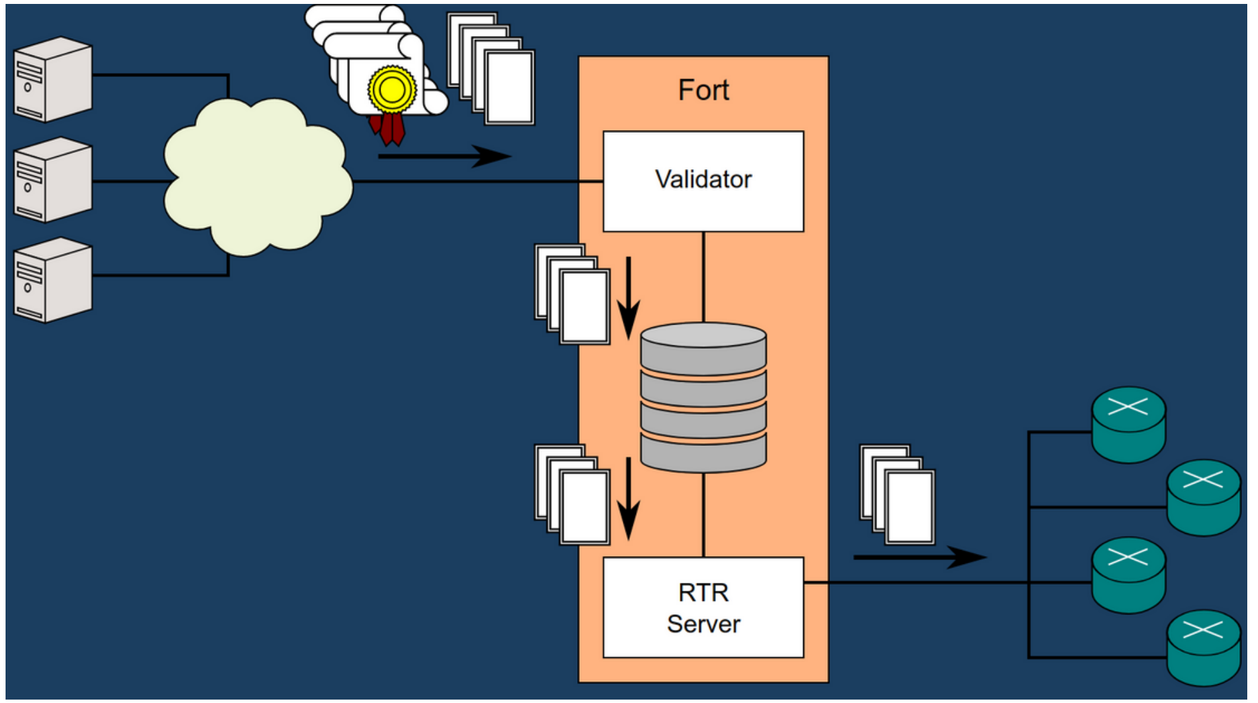
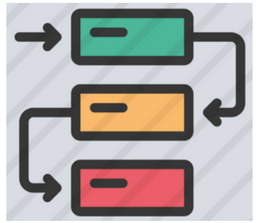


Imagen extraída de https://nicmx.github.io/FORT-validator/intro-fort.html

Fort Paso a Paso

RECETA FRR



PASO 1

Instalar Dependencias

PASO 2

Instalar Librerias

PASO 3

Instalar FRR RPKI

PASO 4

Habilitar Demonios

PASO 5

Iniciar Servicio FRR

Fort Paso a Paso

Fort Paso a Paso

Receta

FRR EN CENTOS7

INSTALAR DEPENDENCIAS

yum install pcre-devel
yum install libssh
yum install libssh-devel
yum install c-ares

INSTALAR LIBRERIAS

Libyang
wget https://ci1.netdef.org/browse/LIBYANG-YANGRELEASE-10/artifact/shared/CentOS-7-x86_64-Packages/
rpm -iUv libyang-0.16.111-0.x86_64.rpm
rpm -iUv libyang-devel-0.16.111-0.x86_64.rpm
Librtr
wget https://ci1.netdef.org/browse/RPKI-RTRLIB-110/artifact/shared/CentOS-7-x86_64-Packages/
rpm -iUv librtr-0.7.0-1.el7.centos.x86_64.rpm
rpm -iUv librtr-devel-0.7.0-1.el7.centos.x86_64.rpm

INSTALAR FRR RPKI

wget https://github.com/FRRouting/frr/releases/tag/frr-7.2/frr-7.2RPKI-01.el7.centos.x86_64.rpm
rpm -iUv frr-7.2RPKI-01.el7.centos.x86_64.rpm

Fort Paso a Paso

Receta

FRR EN CENTOS7

MODIFICAR ARCHIVO DAEMON

nano /etc/frr/daemons

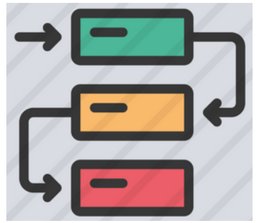
bgpd=yes
ospfd=yes
ospf6d=yes
bgpd_options="   -A 127.0.0.1 -M rpki"

INICIAR SERVICIO

systemctl daemon-reload
systemctl enable frr
systemctl start frr

```
● frr.service - FRRouting
   Loaded: loaded (/usr/lib/systemd/system/frr.service; disabled; vendor preset: disabled)
   Active: active (running) since mar 2020-03-03 18:27:55 -03; 24h ago
     Docs: https://frrouting.readthedocs.io/en/latest/setup.html
  Process: 11472 ExecStop=/usr/lib/frr/frrinit.sh stop (code=exited, status=0/SUCCESS)
  Process: 11502 ExecStart=/usr/lib/frr/frrinit.sh start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/frr.service
           ├─11507 /usr/lib/frr/watchfrr -d zebra bgpd ospfd ospf6d staticd
           ├─11528 /usr/lib/frr/zebra -d -A 127.0.0.1 -s 90000000
           ├─11539 /usr/lib/frr/ospfd -d -A 127.0.0.1
           ├─11542 /usr/lib/frr/ospf6d -d -A ::1
           ├─11545 /usr/lib/frr/staticd -d -A 127.0.0.1
           └─11618 /usr/lib/frr/bgpd -d -A 127.0.0.1 -M rpki
```

RECETA FORT



PASO 1

Instalar Dependencias

PASO 2

Instalar OpenSSL

PASO 3

Instalar GCC

PASO 4

Instalar FORT

PASO 5

Iniciar FORT

Routing Technology for a Free and Open Internet

Fort Paso a Paso

Receta

FORT V1.3.0 CENTOS7

INSTALAR DEPENDENCIAS

yum install autoconf automake git jansson-devel pkgconfig rsync libcurl-devel libxml2-devel make pkgconfig rsync tar wget
yum groupinstall "Development Tools"

INSTALAR OPENSSL

curl https://www.openssl.org/source/openssl-1.1.0k.tar.gz | tar xvz
cd openssl-1.1.0k
./config --prefix=/usr/local --openssldir=/usr/local/openssl
make
sudo make install
sudo mv libcrypto.so.1.1 libssl.so.1.1 /usr/lib64/
sudo ln -sfn /usr/local/bin/openssl /usr/bin/openssl

INSTALAR GCC

Versión igual o superior a 4.9
sudo yum install devtoolset-8-gcc
sudo yum install centos-release-scl epel-release openssl11-devel

Fort Paso a Paso

Receta

FORT V1.3.0 CENTOS7

```
rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0URYSGqUz2myBsOzeW1j
Q6NsxNvlLMyhWknvnl8NiBCs/T/S2XuNKQNZ+wBZxIgPPV2pFBFeQAvoH/WK83Hw
A26V2siwm/MY2nKZ+Olw+wlpzlZ1p3Ipj2eNcKrmit8BwBC8xImzuCGaV0jkRB0G
Z0hoH6Ml03umLprRsn6v0xOP0+l6Qc1ZHMFVFb385IQ7FQQTcVIxrdeMsoyJq9eM
kE6DoclHhF/NlSllXubASQ9KUWqJ0+Ot3QCXr4LXECMfkpkVR2TZT+v5v658bHVs
6ZxRD1b6Uk1uQKAyHUbn/tXvP8lrjAibGzVsXDT2L0x4Edx+QdixPgOji3gBMyL2
VwIDAQAB
```

INSTALAR FORT

scl enable devtoolset-8 bash
cd ~
wget https://github.com/NICMx/FORT-validator/releases/download/v1.3.0/fort-1.3.0.tar.gz
tar xvzf fort-1.3.0.tar.gz
cd fort-1.3.0/
Insertar flags de la nueva versión de OpenSSL
export CFLAGS+=" $(pkg-config --cflags openssl11)" LDFLAGS+="
$(pkg-config --libs openssl11)"
./configure
make
sudo make install
Cerrar la sesión de “devtoolset”
exit

ARCHIVOS TAL

/root/fort-1.3.0/examples/tal
afrinic.tal apnic.tal lacnic.tal ripe.tal
https://www.arin.net/resources/manage/rpki/tal/
arin.tal

Fort Paso a Paso

Receta

FORT V1.3.0 CENTOS7

INICIAR FORT

nano /etc/systemd/system/fort.service

```
[Unit]
Description=FORT
[Service]
Type=simple
ExecStart=/usr/local/bin/fort --mode server --tal /root/fort-1.3.0/examples/tal/ --local-repository /tmp/fort/repository --server.address 200.1.123.151 --server.port 323
[Install]
WantedBy=multi-user.target
```

systemctl enable fort
systemctl start fort

```
[root@sistemas-t1 csanchez]# systemctl status fort
● fort.service - FORT
   Loaded: loaded (/etc/systemd/system/fort.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@sistemas-t1 csanchez]# systemctl start fort
[root@sistemas-t1 csanchez]# systemctl status fort
● fort.service - FORT
   Loaded: loaded (/etc/systemd/system/fort.service; disabled; vendor preset: disabled)
   Active: active (running) since mar 2020-08-04 16:03:36 -04; 2s ago
 Main PID: 16594 (fort)
   CGroup: /system.slice/fort.service
           ├─16594 /usr/local/bin/fort --mode server --tal /root/fort-1.3.0/examples/tal/ --local-repository /tmp/fort/repository ...
           ├─16600 rsync --times --contimeout=20 --timeout=15 --dirs rsync://rpki.afrinic.net/repository/AfriNIC.cer /tmp/fort/rep...
           ├─16602 rsync --times --contimeout=20 --timeout=15 --dirs rsync://rpki.apnic.net/repository/apnic-rpki-root-iana-origin...
           ├─16603 rsync --times --contimeout=20 --timeout=15 --dirs rsync://rpki.arin.net/repository/arin-rpki-ta.cer /tmp/fort/r...
           ├─16604 rsync --times --contimeout=20 --timeout=15 --dirs rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer /tmp/fort/repository...
           ├─16607 rsync --times --contimeout=20 --timeout=15 --dirs rsync://rpki.arin.net/repository/arin-rpki-ta.cer /tmp/fort/r...
           └─16609 rsync --times --contimeout=20 --timeout=15 --dirs rsync://rpki.apnic.net/repository/apnic-rpki-root-iana-origin...

ago 04 16:03:36 sistemas-t1.intra.nic.cl systemd[1]: Started FORT.
```

Receta

FORT V1.3.0
CENTOS7

199.71.0.150 (rpki.arin.net)

Announced By		
Origin AS	**Announcement**	**Description**
AS393220	199.71.0.0/24	ARIN Operations

Captura de tráfico

Observando encabezado IP y TCP al iniciar proceso Fort

tshark -i any port rsync -V

```
    [Bad: False]
    Source: 199.71.0.150 (199.71.0.150)
    Destination: 200.1.123.151 (200.1.123.151)
Transmission Control Protocol, Src Port: rsync (873), Dst Port: 49120 (49120), Seq: 877073, Ack: 345209, Len: 1228
    Source port: rsync (873)
    Destination port: 49120 (49120)
    [Stream index: 5]
    Sequence number: 877073    (relative sequence number)
    [Next sequence number: 878301    (relative sequence number)]
    Acknowledgment number: 345209    (relative ack number)
    Header length: 32 bytes
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
    Window size value: 3147
    [Calculated window size: 201408]
    [Window size scaling factor: 64]
    Checksum: 0x4f00 [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
        No-Operation (NOP)
            Type: 1
                0... .... = Copy on fragmentation: No
                .00. .... = Class: Control (0)
                ...0 0001 = Number: No-Operation (NOP) (1)
        No-Operation (NOP)
            Type: 1
                0... .... = Copy on fragmentation: No
                .00. .... = Class: Control (0)
                ...0 0001 = Number: No-Operation (NOP) (1)
        Timestamps: TSval 606248938, TSecr 3624602396
            Kind: Timestamp (8)
            Length: 10
            Timestamp value: 606248938
            Timestamp echo reply: 3624602396
    [SEQ/ACK analysis]
        [Bytes in flight: 27016]
RSYNC File Synchroniser
    Server Response String: -3847-a923-5bff6fd39646.roa
```

ROAs: Routing Origin Authorization

- Los ROAs contienen información sobre el AS de origen permitido para un conjunto de prefijos
- Los ROAs son firmados usando los certificados generados por RPKI
- Los ROAs firmados son copiados al repositorio

Fort Paso a Paso

Receta

RPKI

INICIAR RPKI

Entrar al router

#vtysh

Configurar Servidor RPKI

#config term

(config)#rpki

(config-rpki)#rpki cache 200.1.123.151 323 preference 1

Iniciar RPKI

#rpki start

```
sistemas-t1.intra.nic.cl# show rpki cache-connection
Connected to group 1
rpki tcp cache 200.1.123.151 323 pref 1
sistemas-t1.intra.nic.cl# show rpki cache-server
host: 200.1.123.151 port: 323
sistemas-t1.intra.nic.cl# show rpki prefix 190.124.24.0/24
Prefix                                  Prefix Length  Origin-AS
190.124.24.0                              23 -  24        27678
sistemas-t1.intra.nic.cl# show rpki prefix 2001:1398:1::/48
Prefix                                  Prefix Length  Origin-AS
2001:1398:1::                             48 -  48        27678
```

Configurar Route-map
R1#config term
R1(config)# route-map RPKI1 permit 10
R1(config-route-map)# match rpki valid

Configurar vecino BGP
R1#config term
R1(config)# router bgp 65501
R1(config-router)# neighbor 200.16.114.23 remote-as 27678

Aplicar Route-map a vecino BGP
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# neighbor 200.16.114.23 route-map RPKI1 in

```
router bgp 65501
 bgp router-id 200.1.123.151
 neighbor 200.1.123.152 remote-as 65501
 neighbor 200.1.123.152 description sistemas-t2
 neighbor 200.16.114.23 remote-as 27678
 neighbor 200.16.114.23 description R2
 neighbor 200.16.114.23 ebgp-multihop 2
 neighbor 2001:1398:376::152 remote-as 65501
 neighbor 2001:1398:376::152 description sistemas-t2
 !
 address-family ipv4 unicast
  neighbor 200.16.114.23 route-map RPKI1 in
  no neighbor 2001:1398:376::152 activate
 exit-address-family
 !
 address-family ipv6 unicast
  neighbor 2001:1398:376::152 activate
 exit-address-family
!
route-map RPKI1 permit 10
 match rpki valid
!
line vty
!
end
sistemas-t1.intra.nic.cl# config term
sistemas-t1.intra.nic.cl(config)# route-map RPKI1 permit 10
sistemas-t1.intra.nic.cl(config-route-map)# match rpki
  invalid   Invalid prefix
  notfound  Prefix not found
  valid     Valid prefix
```

Pruebas

RPKI

Rutas Recibidas antes de aplicar Route Map

```
sistemas-t1.intra.nic.cl# show ip bgp summary

IPv4 Unicast Summary:
BGP router identifier 200.1.123.151, local AS number 65501 vrf-id 0
BGP table version 0
RIB entries 83, using 15 KiB of memory
Peers 2, using 41 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
200.1.123.152   4      65501   13042   13036        0    0    0 01w2d01h            0
200.16.114.23   4      27678      22       4        0    0    0 00:01:02           45

Total number of neighbors 2
```

Rutas Recibidas después de aplicar Route Map

```
sistemas-t1.intra.nic.cl# show ip bgp summary

IPv4 Unicast Summary:
BGP router identifier 200.1.123.151, local AS number 65501 vrf-id 0
BGP table version 0
RIB entries 24, using 4416 bytes of memory
Peers 2, using 41 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
200.1.123.152   4      65501   13045   13040        0    0    0 01w2d01h            0
200.16.114.23   4      27678      42       8        0    0    0 00:04:34           13

Total number of neighbors 2
```

Pruebas

RPKI

Monitoreo con Nagios

Fort Paso a Paso

EN SERVIDOR

nano /etc/nagios/nrpe.cfg

command[check_fort]=/usr/lib64/nagios/plugins/check_procs -C fort -c @0:0

EN NAGIOS

nano /etc/nagios/objects/services/sistemas-t1.cfg

```
define service{
use                     generic-service,graphed-service
host_name               sistemas-t1
service_description     FORT
is_volatile             0
check_period            24x7
max_check_attempts      3
normal_check_interval   2
retry_check_interval    1
contact_groups
notification_interval    240
notification_period      24x7
notification_options     w,u,c,r
check_command            check_remote!check_fort
active_checks_enabled 1
}
```

Monitoreo con Nagios

Service Information
Last Updated: Wed Aug 5 13:01:50 -04 2020
Updated every 90 seconds
Nagios® Core™ 4.0.4 - www.nagios.org
Logged in as *nagiosadmin*

View Information For This Host
View Status Detail For This Host
View Alert History For This Service
View Trends For This Service
View Alert Histogram For This Service
View Availability Report For This Service
View Notifications For This Service

Service
FORT
On Host
sistemas-t1.intra.nic.cl
(sistemas-t1)

Member of
No servicegroups.

200.1.123.151

Service State Information

Current Status:	OK (for 0d 1h 49m 3s)
Status Information:	PROCS OK: 1 process with command name 'fort'
Performance Data:	procs=1;;@0:0;0;
Current Attempt:	1/3 (HARD state)
Last Check Time:	08-05-2020 13:00:47
Check Type:	ACTIVE
Check Latency / Duration:	0,000 / 0,000 seconds
Next Scheduled Check:	08-05-2020 13:02:47
Last State Change:	08-05-2020 11:12:47
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0,00% state change)
In Scheduled Downtime?	NO
Last Update:	08-05-2020 13:01:40 (0d 0h 0m 10s ago)

Fort Paso a Paso

Agosto, 2020

¡GRACIAS!

CELSA SÁNCHEZ
csanchez@nic.cl

FORT PASO A PASO