

Technology Alliance Update Week of September 28 2012



Matt Quill, 2012-28-09

Epic is one of the most important software providers in the healthcare segment of the industry today. Given government mandates and support for Electronic Medical Records over the next decade, the presence of Epic at most hospital and clinical facilities will be essential to adhering to regulatory mandates, increasing the overall efficiency and effectiveness of health care delivery and ensuring that patient history can be rapidly shared between healthcare providers.

As doctors and other clinical staff are increasingly mobile, it is essential that access to patient information can follow from practice to hospital to remote clinic. Epic is the leading provider in the Electronic Medical Records space and ensures that patient information can be reliably accessed anywhere.

We have a happy customer that is willing to provide some of the details of his deployment of Epic Hyperspace. One of the very cool aspects of this deployment is the fact that they used the F5 power of iRules to track the hospital or medical center from which the user is connected. This is important for auditing and (potentially) an internal chargeback mechanism and demonstrates the power of the F5 full proxy architecture. I have to admit that cracking a *ucs to document details of the deployment is not always ideal. As always, please feel free to reach out to me with any details on our joint solution.

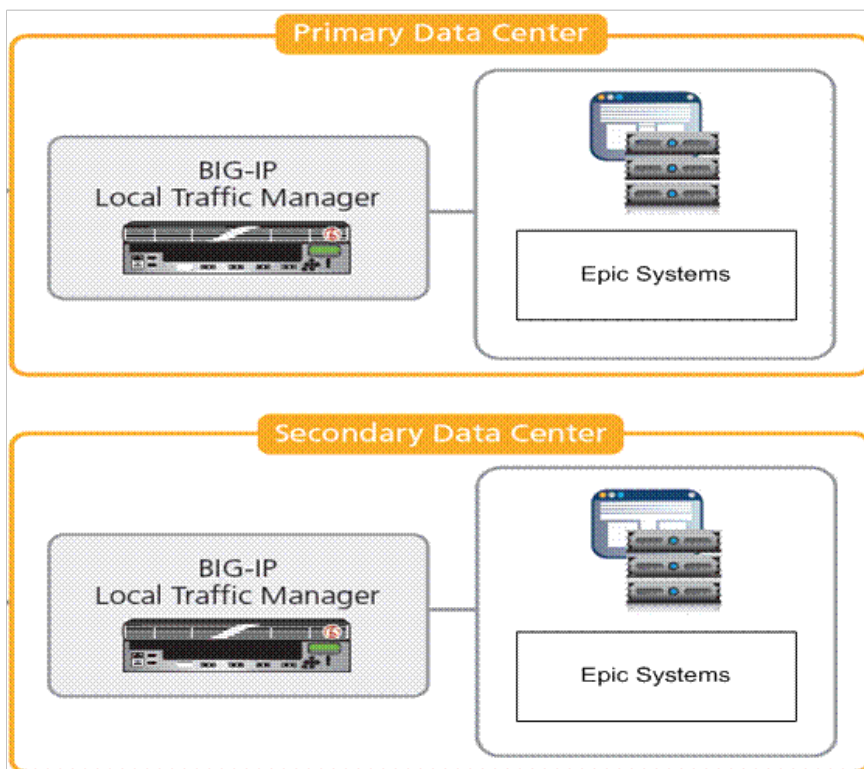


Figure 1: Primary Site 2-8900 LTM Devices, Secondary Site 1 8900 LTM

Setup and Configuration

Platform	Software Version	Products
BIG-IP 8900 x 2	10.2	LTM

For networking setup and configuration of user traffic the 2 10GB interfaces were configured on the F5 devices. We configured a trunk for the two 10GB interfaces providing a full 20GB pipe for incoming client traffic.

The BIG-IP on which this Epic Hyperspace application is deployed has multiple route domains and other application configurations. We will assume that the user has a working knowledge of the basic BIG-IP networking setup and VLAN configuration.

Configuration of VLANS and Networking

1. Setup and Configuration of Network Trunk on 8900

```
{  
trunk XX-L1-GOPS_CHANNEL19 {  
lacp enable  
interfaces {  
3.1  
3.2  
}  
}
```

2. Configure VLAN for Epic Deployment and Associate it with Trunk

vlan VLAN104_EPIC {

```
tag 104  
mac masq 02:01:D7:B7:2A:04  
failsafe enable  
timeout 30  
failsafe failover  
trunks tagged XX-L1-GOPS_CHANNEL19  
}  
route domain 1 {  
description "RD1-XXX_EPIC"  
vlans VLAN104_EPIC  
}
```

3. Configure Self-IPs

```
}  
self 172.27.104.248%1 {  
netmask 255.255.255.0  
vlan VLAN104_EPIC  
allow default  
}
```

4. Configure Epic Specific Monitors

```
monitor EPIC_ECP_COMM {  
defaults from tcp  
timeout 11  
dest *:20300
```

partition P1-XXX_EPIC

}

monitor EPIC_ECP_PROBE {

defaults from tcp

timeout 11

dest *:20110

partition P1-XXX_EPIC

}

monitor EPIC_MOBILE_HAIKU_KHWPEPC001 {

defaults from http

partition P1-XXX_EPIC

recv "Interconnect Service:

RunningStatus\" class=\"running\">Running"

send "GET /interconnect-haiku/default.aspx HTTP/1.1\r\nHost: xxxpepc001.xxx

ealth.com\r\nConnection: Close\r\n\r\n"

}

monitor EPIC_MOBILE_HAIKU_XXXPEPC002 {

defaults from http

partition P1-XXX_EPIC

recv "Interconnect Service:

RunningStatus\" class=\"running\">Running"

send "GET /interconnect-haiku/default.aspx HTTP/1.1\r\nHost: xxxpepc002.ketth

ealth.com\r\nConnection: Close\r\n\r\n"

}

monitor EPIC_MOBILE_INTER_XXXPEPC001 {

defaults from http

partition P1-XXX_EPIC

recv "OLTP Server Status: UP

an>"

send "GET /interconnect-haiku/default.aspx HTTP/1.1\r\nHost: xxxpepc001.xxxth

ealth.com\r\nConnection: Close\r\n\r\n"

}

monitor EPIC_MOBILE_INTER_XXXPEPC002 {

defaults from http

partition P1-XXX_EPIC

recv "OLTP Server Status: UP

```
an>"
```

```
send "GET /interconnect-haiku/default.aspx HTTP/1.1\r\nHost: xxxpepc002.xxxth
```

```
ealth.com\r\nConnection: Close\r\n\r\n"
```

```
}
```

```
monitor EPIC_PRINT_COMM {
```

```
defaults from ftp
```

```
partition P1-XXX_EPIC
```

```
}
```

```
monitor EPIC_PRINT_PROBE_FTP {
```

```
defaults from tcp
```

```
dest *:ftp
```

```
partition P1-XXX_EPIC
```

```
}
```

```
monitor EPIC_TEST_MONITOR {
```

```
defaults from tcp
```

```
dest *:ms-wbt-server
```

```
partition P1-XXX_EPIC
```

```
}
```

```
monitor test1 {
```

```
defaults from tcp
```

```
partition P1-XXX_EPIC
```

```
recv "220"
```

```
send "ftp://xxx.xx.xxx.xxx"
```

```
}
```

```
monitor test2 {
```

```
defaults from tcp
```

```
dest *:ftp
```

```
partition P1-XXX_EPIC
```

```
}
```

5. Configure SNAT Pools (Note Only Necessary for Larger Configurations Exceeding 64K Simultaneous Connections, SNAT pools in this instance will be used to log the location of the user)

```
snatpool BK_SNAT_POOL {
```

```
members 172.27.104.224%1
```

```
}
```

```
snatpool DR_SNAT_POOL {
```

```
members 172.27.104.126%1
```

```
}  
  
snatpool FH_SNAT_POOL {  
members 172.27.104.123%1  
}  
  
snatpool GM_SNAT_POOL {  
members 172.27.104.124%1  
}  
  
snatpool GV_SNAT_POOL {  
members 172.27.104.130%1  
}  
  
snatpool XX_SNAT_EPIC_MOBILE {  
members 172.27.104.181%1  
  
snatpool XX_SNAT_POOL {  
members 172.27.104.127%1  
}  
  
snatpool XX_SNAT_PRINT {  
members 172.27.104.231%1  
}  
  
snatpool RS_SNAT_POOL {  
members 172.27.104.128%1  
}  
  
snatpool SH_SNAT_POOL {  
members 172.27.104.125%1  
}  
  
snatpool SV_SNAT_POOL {  
members 172.27.104.129%1  
}  
  
snatpool UNKNOWN_SNAT_POOL {  
members 172.27.104.118%1  
}  
}
```

6. Configure Epic Test Profiles

```
profile tcp EPIC_TEST_Profile {  
defaults from tcp-lan-optimized  
idle timeout 7200
```

7. Add Nodes to Configuration

```
node 172.27.104.20%1 {
monitor EPIC_ECP_PROBE
screen XXXPX010
}
node 172.27.104.21%1 {
monitor EPIC_ECP_PROBE
screen XXXPX011
}
node 172.27.104.22%1 {
monitor EPIC_ECP_PROBE
screen XXXPX012
}
node 172.27.104.23%1 {
monitor EPIC_ECP_PROBE
screen XXXPX013
}
node 172.27.104.24%1 {
monitor EPIC_ECP_PROBE
screen XXXPX014
}
node 172.27.104.25%1 {
monitor EPIC_ECP_PROBE
screen XXXPX015
}
node 172.27.104.26%1 {
monitor EPIC_ECP_PROBE
screen XXXPX016
}
node 172.27.104.37%1 {
monitor EPIC_ECP_PROBE
screen XXXPX019
}
node 172.27.104.183%1 {
monitor EPIC_ECP_PROBE
screen XXXPX009
}
```

```
pool EPIC_ECP_POOL {
```

```
lb method member least conn
```

```
monitor all EPIC_ECP_COMM
```

```
members {
```

```
172.27.104.20%1:20300 {
```

```
monitor EPIC_ECP_COMM
```

```
}
```

```
172.27.104.21%1:20300 {
```

```
monitor EPIC_ECP_COMM
```

```
}
```

```
172.27.104.22%1:20300 {
```

```
monitor EPI }
```

```
172.27.104.23%1:20300 {
```

```
monitor EPIC_ECP_COMM
```

```
}
```

```
172.27.104.24%1:20300 {
```

```
monitor EPIC_ECP_COMM
```

```
}
```

```
172.27.104.25%1:20300 {
```

```
monitor EPIC_ECP_COMM
```

```
}
```

```
172.27.104.26%1:20300 {
```

```
monitor EPIC_ECP_COMM
```

```
}
```

```
172.27.104.37%1:20300 {
```

```
monitor EPIC_ECP_COMM
```

```
}
```

```
172.27.104.183%1:20300 {
```

```
monitor EPIC_ECP_COMM
```

```
}
```

```
}
```

```
}
```

8. Configure Pools

```
pool EPIC_INT_INTERCONN_POOL1 {
```

```
lb method least connC_ECP_COMM
```

```
members {
```

172.27.104.177%1:http {

monitor gateway_icmp

}

172.27.104.178%1:http {

monitor gateway_icmp

}

}

}

pool **EPIC_INT_MOBILE_POOL1** {

lb method least conn

members {

172.27.104.169%1:http {

monitor EPIC_MOBILE_HAIKU_XXXPEPC001 and EPIC_MOBILE_INTER_XXXPEPC001

}

172.27.104.170%1:http {

monitor EPIC_MOBILE_HAIKU_XXXPEPC002 and EPIC_MOBILE_INTER_XXXPEPC002

}

}

}

pool **EPIC_PRINT_POOL1** {

monitor all EPIC_PRINT_PROBE_FTP

members {

172.27.104.172%1:ftp {}

172.27.104.173%1:ftp {}

172.27.104.174%1:ftp {}

172.27.104.176%1:ftp {}

}

}

pool EPIC_PRINT_POOL2 {

monitor all EPIC_PRINT_PROBE_FTP

members {

172.27.104.155%1:ftp {}

172.27.104.156%1:ftp {}

172.27.104.171%1:ftp {

monitor EPIC_PRINT_PROBE_FTP

}


```

}
}
pool EPIC_PRINT_POOL3 {
monitor all EPIC_PRINT_PROBE_FTP
members {
172.27.104.171%1:ftp {}
172.27.104.172%1:ftp {}
172.27.104.173%1:ftp {}
172.27.104.174%1:ftp {}
}
}

```

```

pool EPIC_TEST_POOL {
lb method member least conn
monitor all EPIC_TEST_MONITOR
members {
172.27.104.202%1:ms-wbt-server {}
172.27.104.206%1:ms-wbt-server {
monitor EPIC_TEST_MONITOR
}
}
}

```

9. Configure iRule to Identify Client Location and Log User IP Address

```

rule IRULE-XXX_EPIC_PROD {
# Location Selective SNAT
# CPU impact: Minimal
# Requirement: - Match Client IP to identify Client location & give proper SNAT address
#
# If client and server are on the same IP network,
# invoke SNAT to prevent IP routed triangulation.
when CLIENT_ACCEPTED {
##Start TCP timer
set tcp_start_time "[clock clicks -milliseconds]"
set LB_SRV "[getfield [IP::local_addr] "%" 1]"
set SRC "[getfield [IP::remote_addr] "%" 1]"
if {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.24.0.0/17]} {
use snatpool GM_SNAT_POOL

```

```
set location "XXX"

STATS::incr Location_XXXXXXXXXX

}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.24.128.0/17]}

{

use snatpool BK_SNAT_POOL

set location "XXX"

STATS::incr Location_Stats XXXX_Medical_Center

}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.25.0.0/16]} {

use snatpool SH_SNAT_POOL

set location "XXX"

STATS::incr Location_Stats XXXXX_Medical_Center

}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.26.0.0/17]} {

use snatpool DR_SNAT_POOL

set location "XX"

STATS::incr Location_Stats Disaster_Recovery_Center

}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.27.0.0/16]} {

use snatpool XX_SNAT_POOL

set location "XXX"

STATS::incr Location_Stats XXXXX_Medical_Center

}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.28.0.0/16]} {

use snatpool RS_SNAT_POOL

set location "REMOTE"

STATS::incr Location_Stats XXX_Remote_Sites

}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.29.0.0/16]} {

use snatpool SV_SNAT_POOL

set location "XXX"

STATS::incr Location_Stats XXXXXXX_Medical_Center

}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.30.0.0/16]} {

use snatpool XX_SNAT_POOL
```

```

set location "XXX"

STATS::incr Location_Stats XXXXXX_Medical_Center
}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.23.0.0/16]} {

use snatpool FH_SNAT_POOL

set location "XXX"

STATS::incr Location_Stats XXXXXXXXXX_Hospital

}

else {

use snatpool UNKNOWN_SNAT_POOL

set location "UNKNOWN"

STATS::incr Location_Stats Unknown_Addresses

}

}

when SERVER_CONNECTED {

set RTT "[expr [clock clicks -milliseconds] - $tcp_start_time]"

##End TCP timer

set SRC_NAT "[getfield [IP::local_addr] "%" 1]"

set REAL_SRV "[getfield [IP::server_addr] "%" 1]"

set DEST_PORT "[TCP::server_port]"

##Src-ClientIP, SRC_NAT-SNAT IP, LB_SRV-VIP, REAL_SRV-Node, DEST_PORT-TCP Po

rt, RTT-TCP Timer time

log -noname local0. "PART=P1-KHN_EPIC, LOCATION=$location, SRC=$SRC, SRC_NAT

=$SRC_NAT, LB_SRV=$LB_SRV, REAL_SRV=$REAL_SRV, DEST_PORT=$DEST_PORT, RTT=$RTT ms

,"

}

}

rule IRULE-XXX_EPIC_TEST {

# Location Selective SNAT

# CPU impact: Minimal

# Requirement: - Match Client IP to identify Client location & give proper SNAT address

#

# If client and server are on the same IP network,

# invoke SNAT to prevent IP routed triangulation.

when CLIENT_ACCEPTED {

##Start TCP timer

```

```
set tcp_start_time "[clock clicks -milliseconds]"
set LB_SRV "[getfield [IP::local_addr] "%" 1]"
set SRC "[getfield [IP::remote_addr] "%" 1]"
if {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.24.0.0/17]} {
use snatpool GM_SNAT_POOL
set location "XXX"
STATS::incr Location_Stats XXXXXX_Memorial_Hospital
}
elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.24.128.0/17]}
{
use snatpool BK_SNAT_POOL
set location "XXX"
STATS::incr Location_Stats XXXXXXXX_Medical_Center
}
elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.25.0.0/16]} {
use snatpool SH_SNAT_POOL
set location "XXX"
STATS::incr Location_Stats XXXXXXXX_Medical_Center
}
elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.26.0.0/17]} {
use snatpool DR_SNAT_POOL
set location "DR"
STATS::incr Location_Stats Disaster_Recovery_Center
}
elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.27.0.0/16]} {
use snatpool XX_SNAT_POOL
set location "XXX"
STATS::incr Location_Stats XXXXXX_Medical_Center
}
elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.28.0.0/16]} {
use snatpool RS_SNAT_POOL
set location "REMOTE"
STATS::incr Location_Stats KHN_Remote_Sites
}
elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.29.0.0/16]} {
use snatpool SV_SNAT_POOL
```

```

set location "XXX"

STATS::incr Location_Stats XXXXXXXXX_Medical_Center
}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.30.0.0/16]} {

use snatpool GV_SNAT_POOL

set location "XXX"

STATS::incr Location_Stats XXXXXXXXX_Medical_Center

}

elseif {[IP::addr [getfield [IP::remote_addr] "%" 1] equals 172.23.0.0/16]} {

use snatpool FH_SNAT_POOL

set location "XXX"

STATS::incr Location_Stats XXXXXXXXX_Hospital

}

else {

use snatpool UNKNOWN_SNAT_POOL

set location "UNKNOWN"

STATS::incr Location_Stats Unknown_Addresses

}

}

when SERVER_CONNECTED {

set RTT "[expr [clock clicks -milliseconds] - $tcp_start_time]"

##End TCP timer

set SRC_NAT "[getfield [IP::local_addr] "%" 1]"

set REAL_SRV "[getfield [IP::server_addr] "%" 1]"

set DEST_PORT "[TCP::server_port]"

##Src-ClientIP, SRC_NAT-SNAT IP, LB_SRV-VIP, REAL_SRV-Node, DEST_PORT-TCP Po
rt, RTT-TCP Timer time

log -noname local0. "PART=P1-KHN_EPIC, LOCATION=$location, SRC=$SRC, SRC_NAT
=$SRC_NAT, LB_SRV=$LB_SRV, REAL_SRV=$REAL_SRV, DEST_PORT=$DEST_PORT, RTT=$RTT ms
,"
}

}

```

10. Configure Additional Virtual Server

```

virtual VS_EPIC_ECP_PROD {

mirror enable

snat automap

```

```
pool EPIC_ECP_POOL
```

```
destination 172.27.104.100%1:20300
```

```
ip protocol tcp
```

```
rules IRULE-XXX_EPIC_PROD (Note the use of the iRule for logging location: Not necessary for basic deployment)
```

```
profiles {
```

```
EPIC_ECP_FASTL4 {}
```

```
Location_Stats {}
```

```
}
```

```
vlangs VLAN104_EPIC enable
```

```
}
```

11. Configure Virtual Server Epic Interconnection1

```
virtual VS_EPIC_INT_INTERCONN1 {
```

```
snatpool XX_SNAT_EPIC_MOBILE
```

```
pool EPIC_INT_INTERCONN_POOL1
```

```
destination 172.27.104.185%1:http
```

```
ip protocol tcp
```

```
profiles fasthttp {}
```

```
vlangs VLAN104_EPIC enable
```

```
}
```

12. Configure Epic Mobile 1

```
virtual VS_EPIC_INT_MOBILE1 {
```

```
snatpool XX_SNAT_EPIC_MOBILE
```

```
pool EPIC_INT_MOBILE_POOL1
```

```
destination 172.27.104.180%1:http
```

```
ip protocol tcp
```

```
profiles fasthttp {}
```

```
vlangs VLAN104_EPIC enable
```

```
}
```

13. Configure Epic Print Production 1

```
virtual VS_EPIC_PRINT_PROD1 {
```

```
translate service disable
```

```
srcport change
```

```
snatpool XX_SNAT_PRINT
```

```
pool EPIC_PRINT_POOL1
```

```
destination 172.27.104.101%1:ftp
```

```
ip protocol tcp

profiles {

ftp {}

tcp-lan-optimized {}

}

vlans VLAN104_EPIC enable

}
```

14. Configure Epic Print Virtual Server

```
virtual VS_EPIC_PRINT_PROD2 {

translate service disable

srcport change

snatpool XX_SNAT_PRINT

pool EPIC_PRINT_POOL2

destination 172.27.104.102%1:ftp

ip protocol tcp

profiles {

ftp {}

tcp {

clientside

}

}

tcp-lan-optimized {

serverside

}

}

vlans VLAN104_EPIC enable

}
```

15. Configure Epic Print Production 3 Virtual Server

```
virtual VS_EPIC_PRINT_PROD3 {

translate service disable

snatpool XX_SNAT_PRINT

pool EPIC_PRINT_POOL3

destination 172.27.104.103%1:ftp

ip protocol tcp

profiles {

ftp {}

tcp-lan-optimized {}

}
```

}

}

16. Configure Virtual Server Epic Test XP

```
virtual VS_EPIC_TEST_XP {  
  mirror enable  
  snat automap  
  pool EPIC_TEST_POOL  
  destination 172.27.104.102%1:ms-wbt-server  
  ip protocol tcp  
  rules IRULE-XXX_EPIC_TEST  
  profiles {  
    EPIC_ECP_FASTL4 {}  
    Location_Stats {}  
  }  
  vlans VLAN104_EPIC enable  
}  
  
pool EPIC_MOBILE_POOL1 {  
  members {  
    204.110.18.241%4:https {  
      monitor EPIC_MOBILE_XXWPEPC003_Monitor  
    }  
    204.110.18.242%4:https {  
      session user disabled  
      monitor EPIC_MOBILE_XXWPEPC004_Monitor  
    }  
  }  
}
```

17. Configure Epic EXT Mobile 1 Virtual Server

```
virtual VS_EPIC_EXT_MOBILE1 {  
  snatpool SNAT_EPIC_MOBILE  
  pool EPIC_MOBILE_POOL1  
  destination 204.110.18.247%4:https  
  ip protocol tcp  
  profiles fasthttp {}  
  vlans VLAN555_EDMZ enable
```


external path cost 20000

VLAN Configuration:

```
vlans {  
  
VLAN104_EPIC  
  
VLAN105_UNIT1  
  
VLAN106_UNIT2  
  
VLAN10_IDMZ  
  
VLAN112_UNIT1  
  
VLAN116_UNIT2  
  
VLAN555_EDMZ  
  
VLAN98_MANG  
  
peerNet  
  
}
```

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com