

Enhanced IP and OpenFlow Switching to Provide Zero Touch Traffic Engineering

Tomorrow's Networks
Implemented
Today

By Dr. William Chimiak
LTS

Overview

Using Northbound Applications with Enhanced IP the following can now be done:

- Flow types can be identified
- moved to ports that provide automatic traffic engineering, and
- Identified by DNS entry to provide traffic engineering throughout the Internet.

How This Will Work

- The Northbound Application (NB App) communicates with the controller
- This combination programs the network infrastructure for a set of traffic engineering functions including network security
- The controlled network infrastructure is optimized for the traffic flows the NB Apps manage.
- Placing flows to particular ports with EnIP NATs attached allows a domain name to be attached
- This enables the network to optimize the entire path throughout the Internet.

Creating the OpenFlow EnIP Network

Set up the Northbound OpenFlow Applications

The OpenFlow switches are now

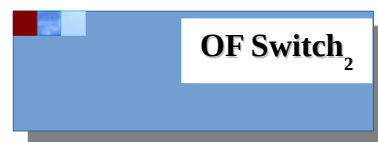
NB App makes a secure socket layer connection

NB App
Mal-Dtect

NB App
Tsunami

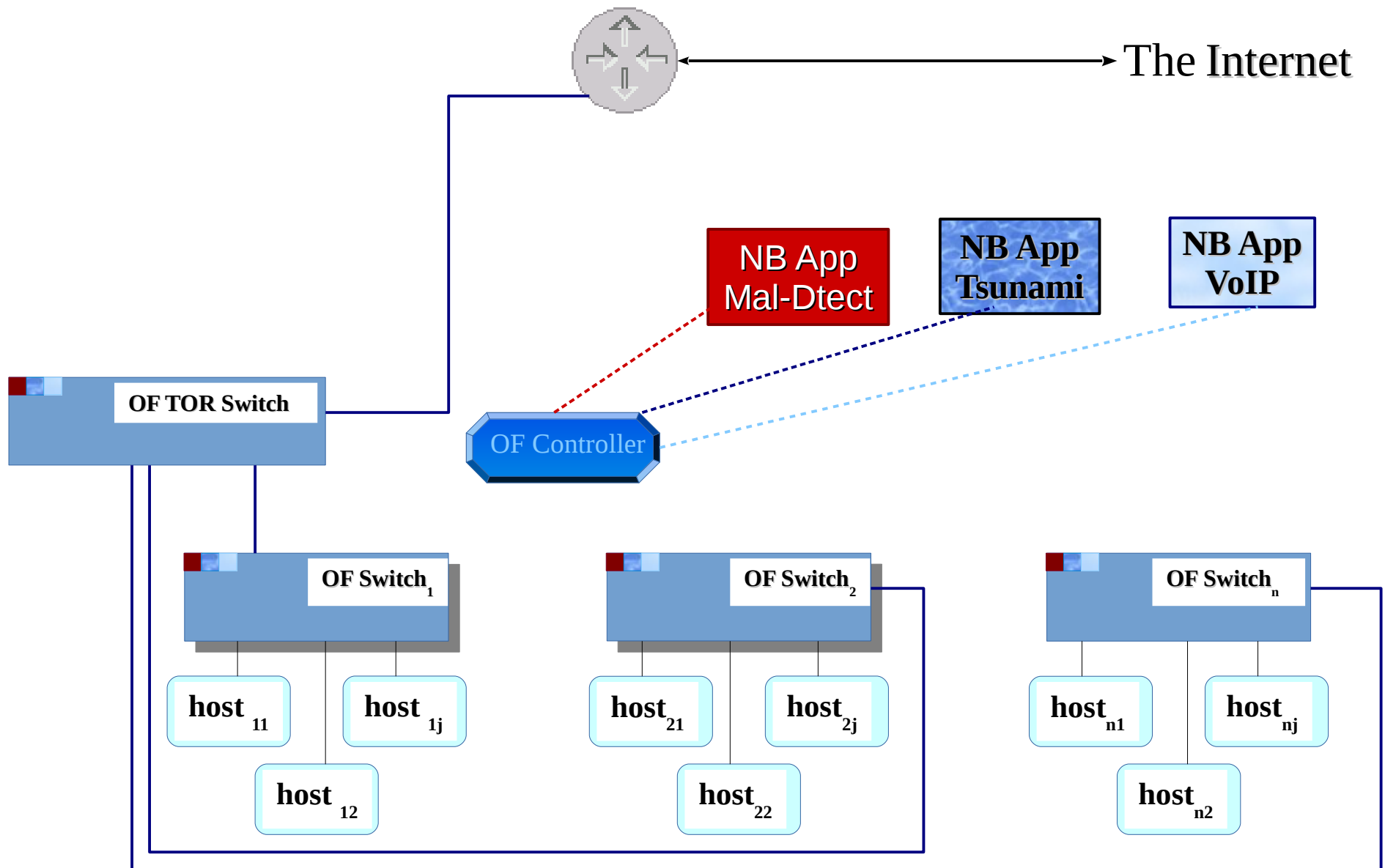
NB App
VoIP

- the malware detection,
- Tsunami mitigation, and
- VoIP optimization mechnism.

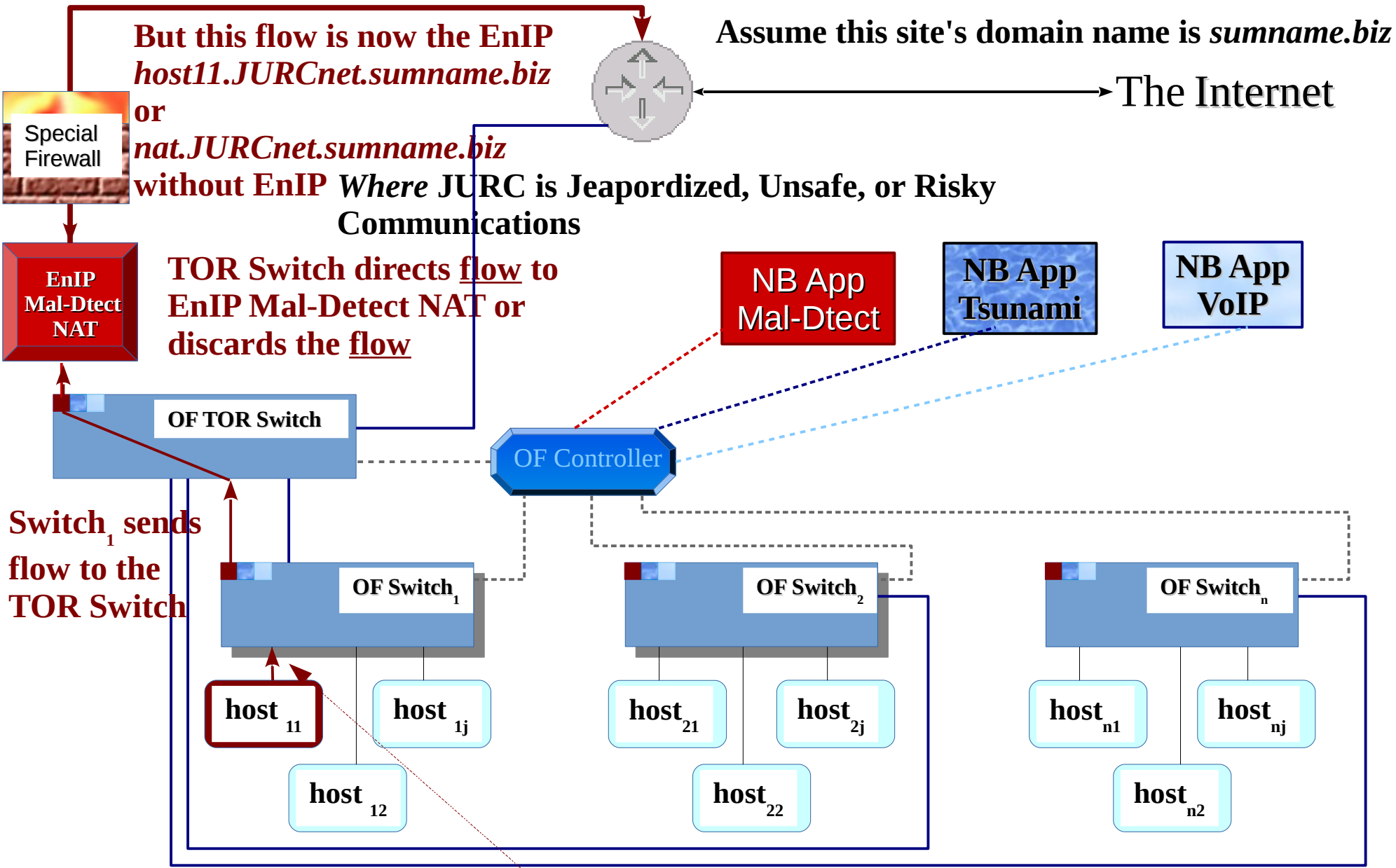


Controller send match/action pairs for flows to the switches

Connect OpenFlow Switch to the Internet



Response to Known Bad Traffic



But this flow is now the EnIP
host11.JURCnet.sumname.biz
 or
nat.JURCnet.sumname.biz
 without EnIP

Assume this site's domain name is *sumname.biz*

The Internet

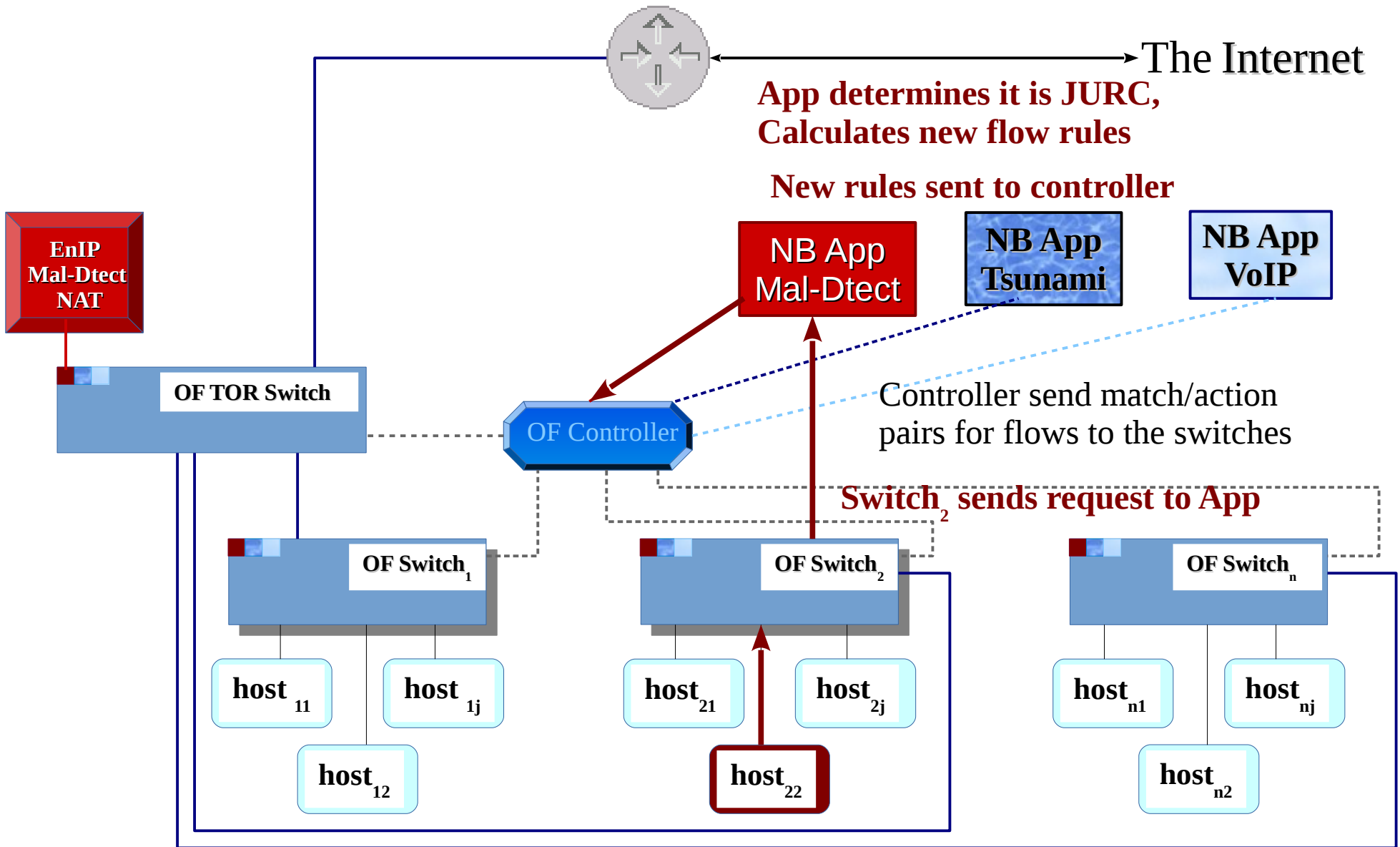
Where JURC is Jeopardized, Unsafe, or Risky
 Communications

TOR Switch directs flow to
 EnIP Mal-Detect NAT or
 discards the flow

Switch₁ sends
 flow to the
 TOR Switch

Bad traffic is generated by host₁₁

Response to Suspicious Traffic Pt 1



Suspicious traffic is generated by host₂₂

Response to Suspicious Traffic (cont'd)

Assume this site's domain name is *sumname.biz*

The Internet

But this flow is now the EnIP
host22.JURCnet.sumname.biz
or
nat.JURCnet.sumname.biz
without EnIP

Where JURC is Jeopardized, Unsafe, or Risky
Communications

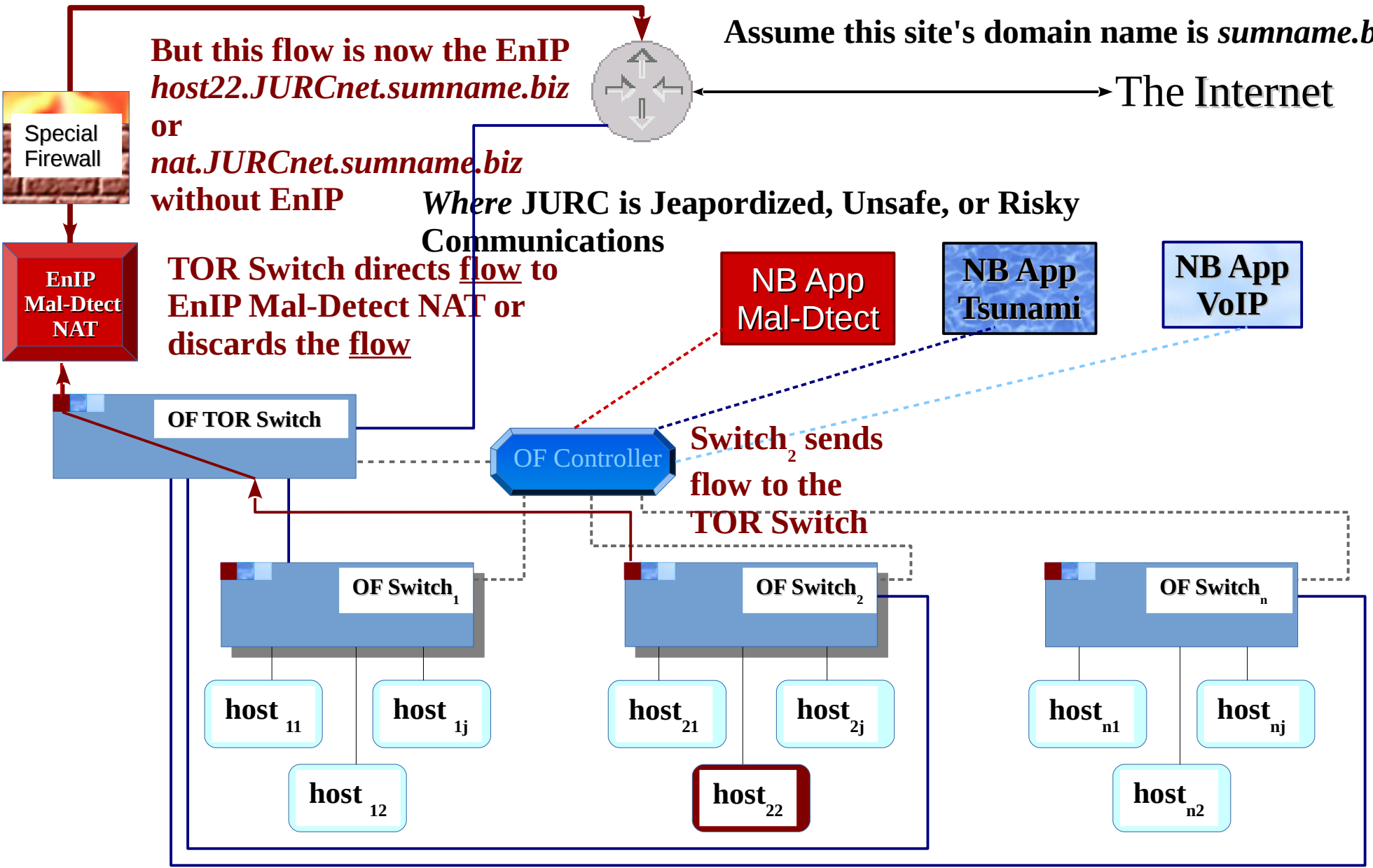
TOR Switch directs flow to
EnIP Mal-Detect NAT or
discards the flow

NB App
Mal-Dtect

NB App
Tsunami

NB App
VoIP

Switch₂ sends
flow to the
TOR Switch



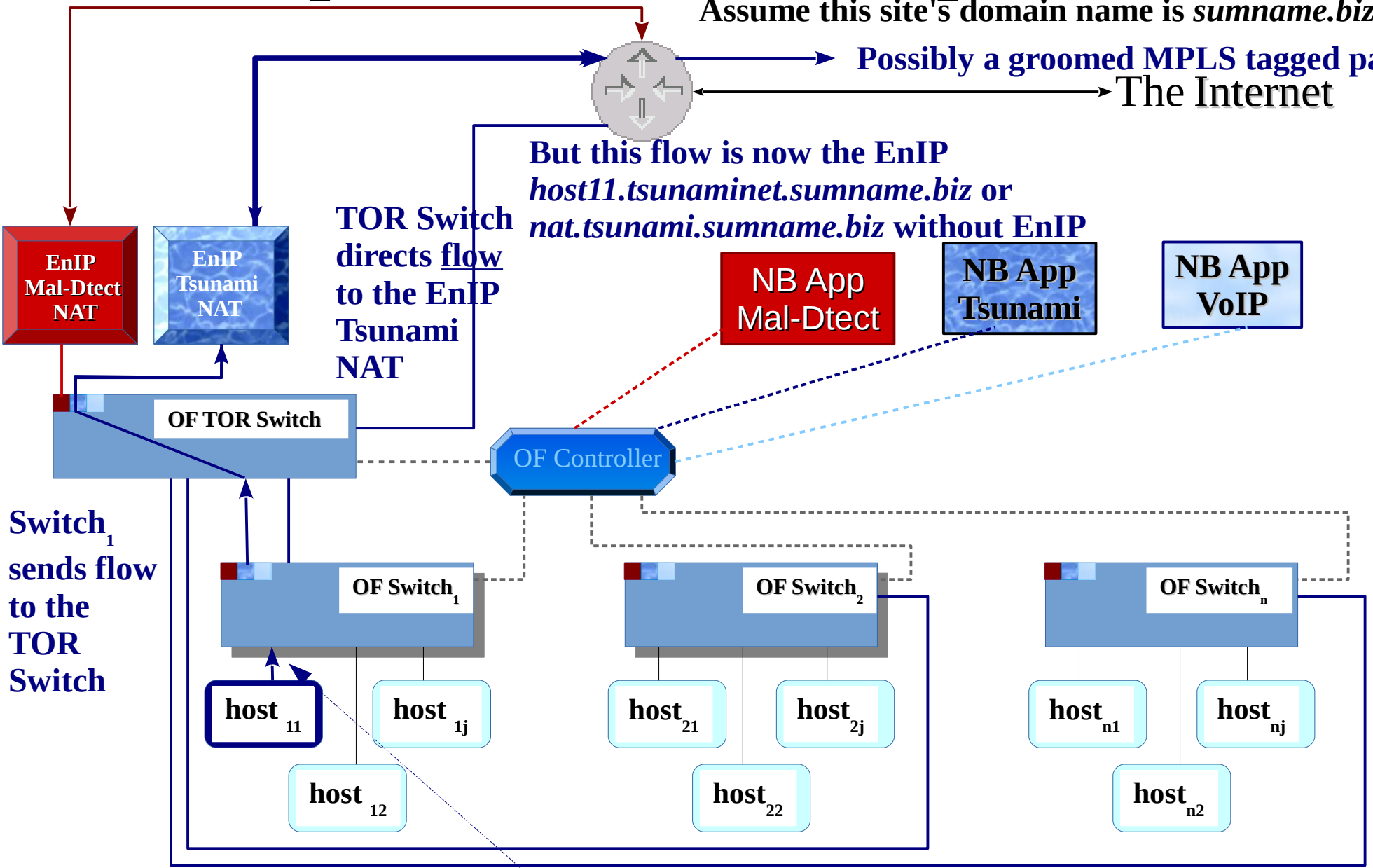
Response to Known Elephant Flow

Assume this site's domain name is *sumname.biz*

Possibly a groomed MPLS tagged path

The Internet

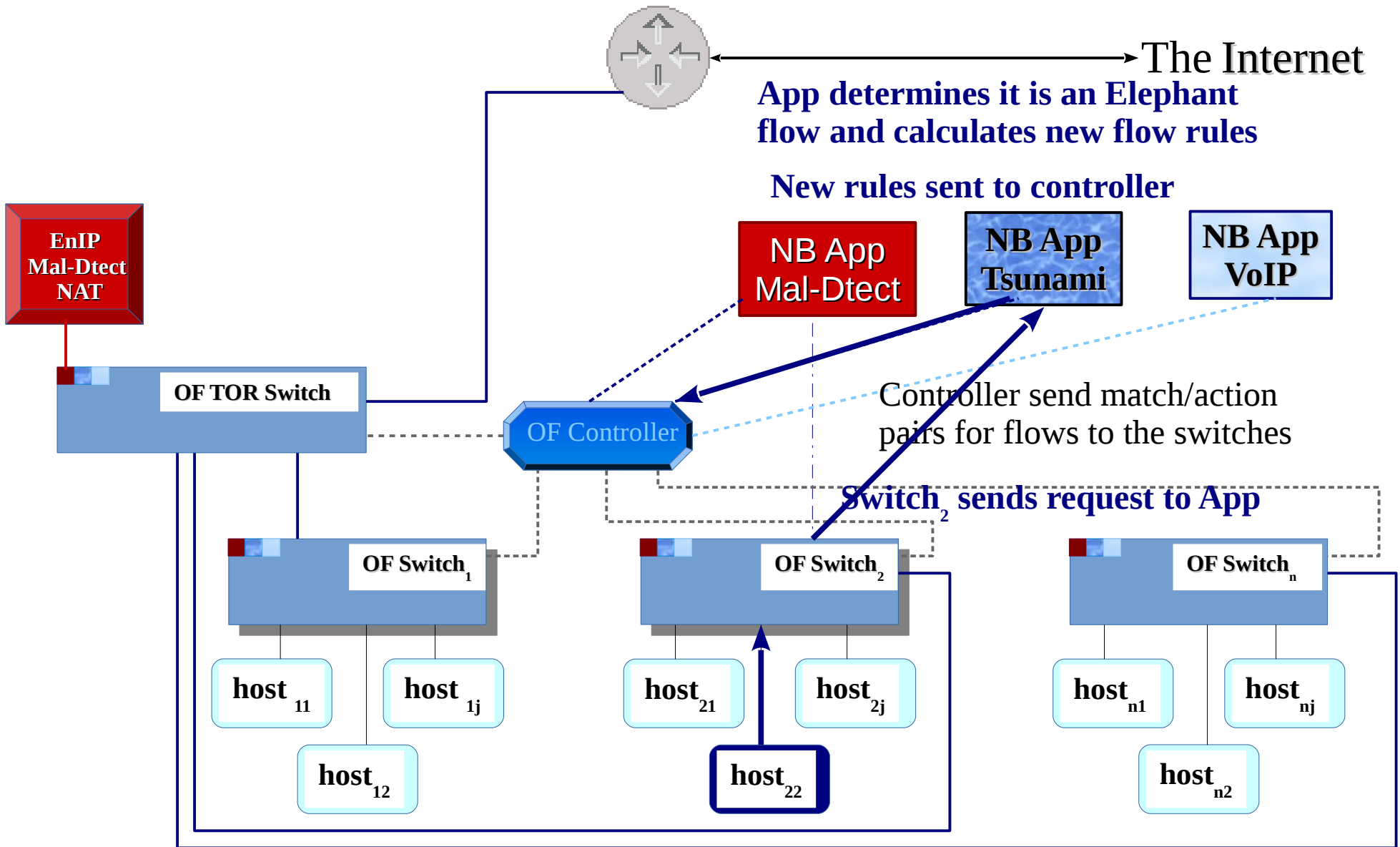
But this flow is now the EnIP
host11.tsunami.net.sumname.biz or
nat.tsunami.sumname.biz without EnIP



Switch₁ sends flow to the TOR Switch

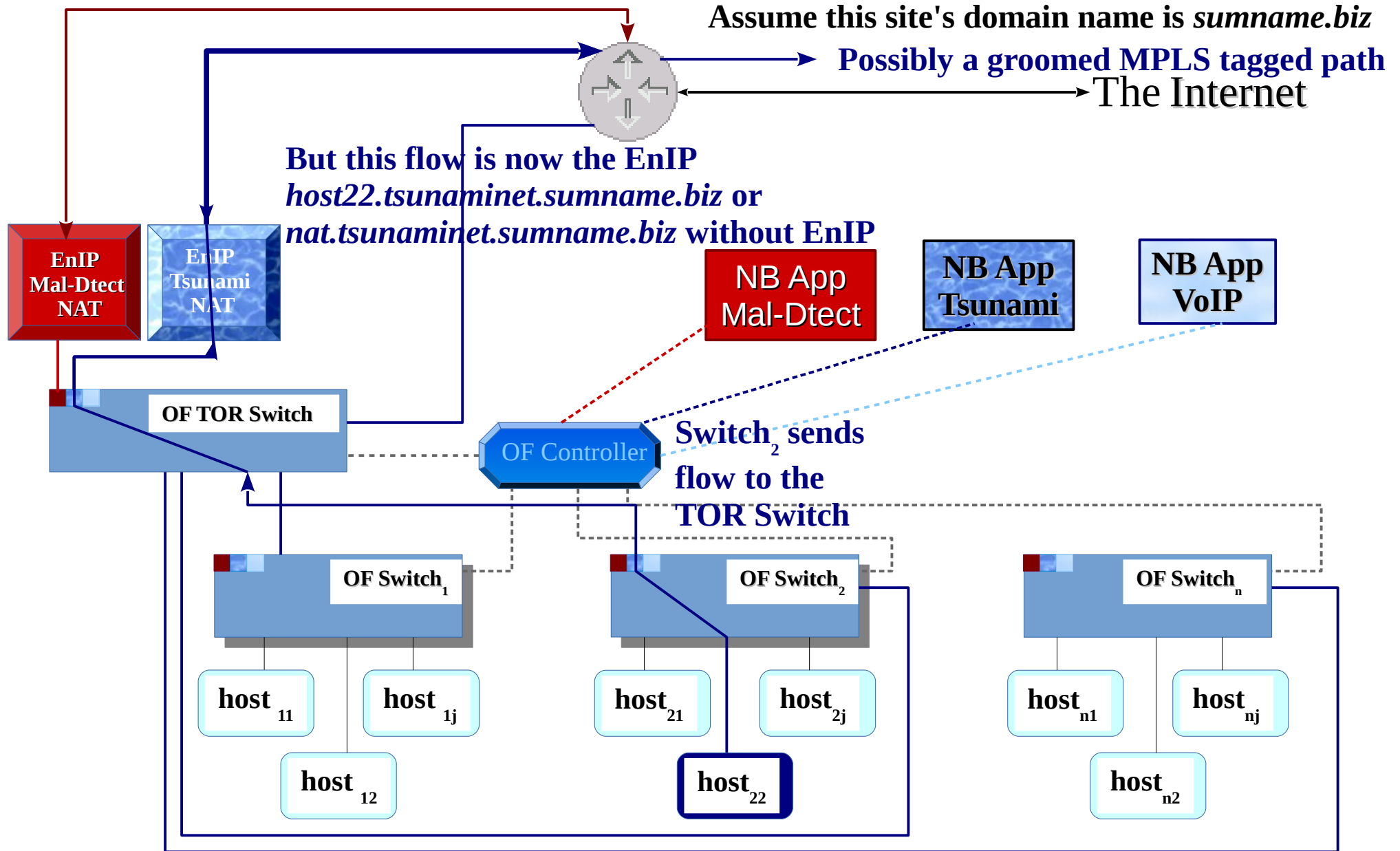
Elephant Flow is requested by host₁₁

Response to suspected Elephant Flow Pt 1

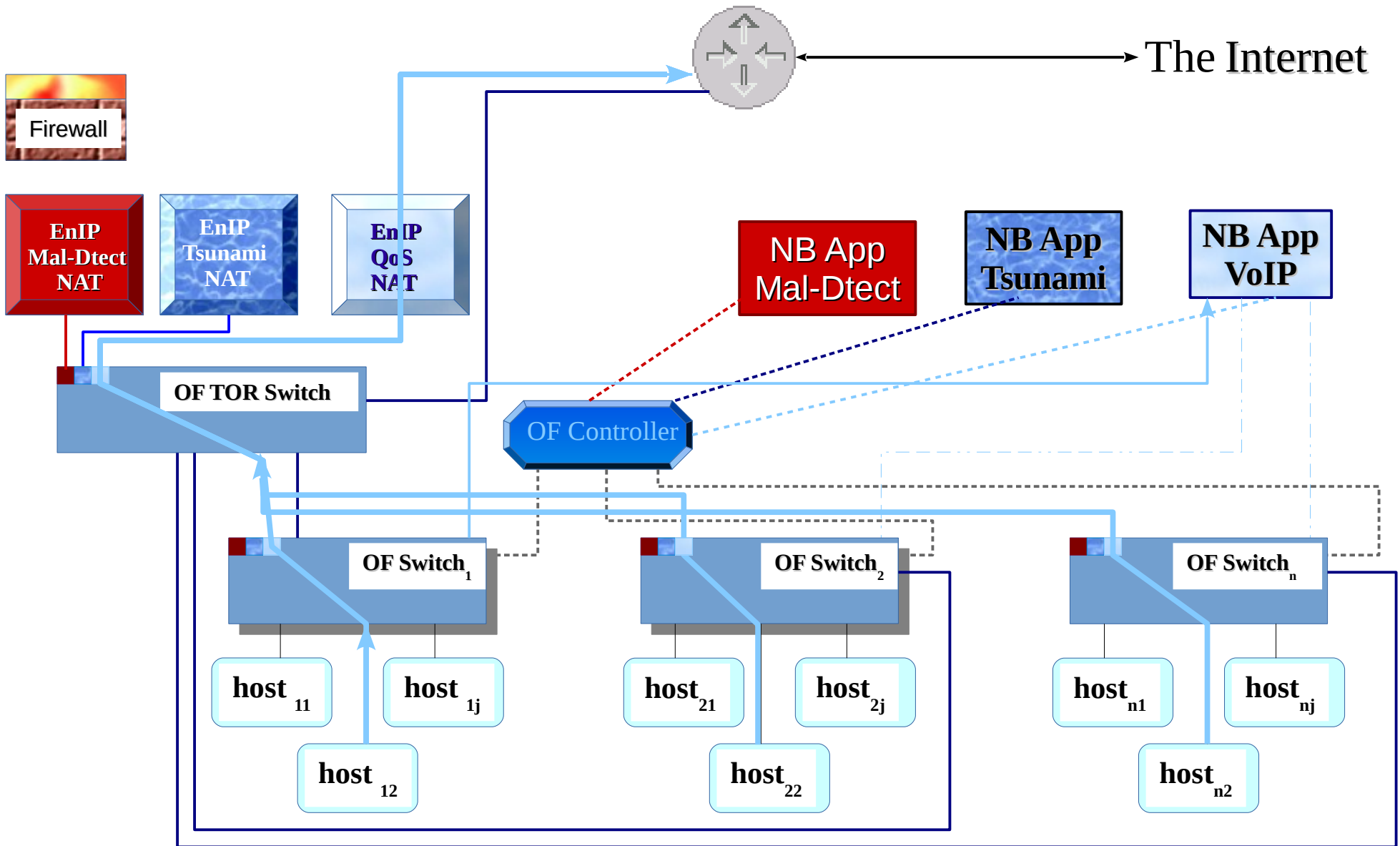


Suspect Elephant Flow is requested by $host_{22}$

Response to suspected Elephant Flow (cont'd)



OpenFlow EnIP Network for VoIP



OpenFlow EnIP Network

