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:

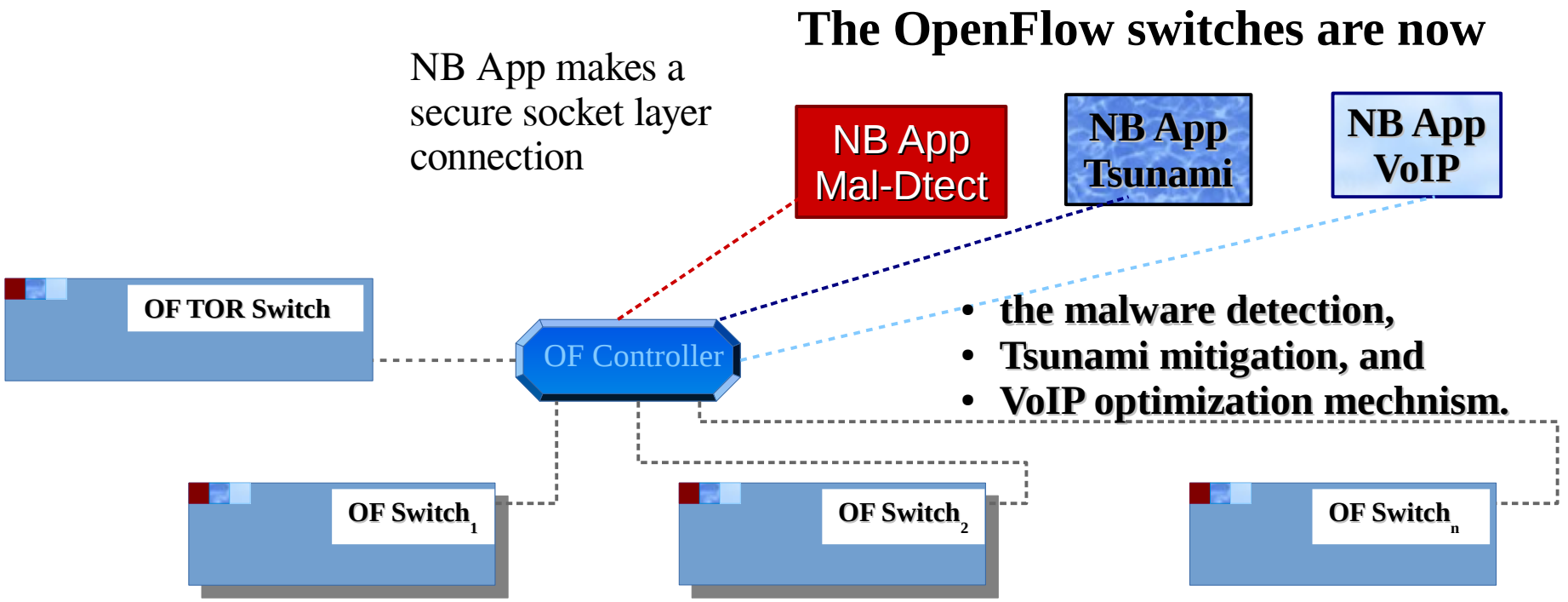
- Flow types can be identified
- moved to ports that provide automatic traffic engineering, and
- Identified by DNS entry to provide traffic engineering throughout the Internet.

How This Will Work

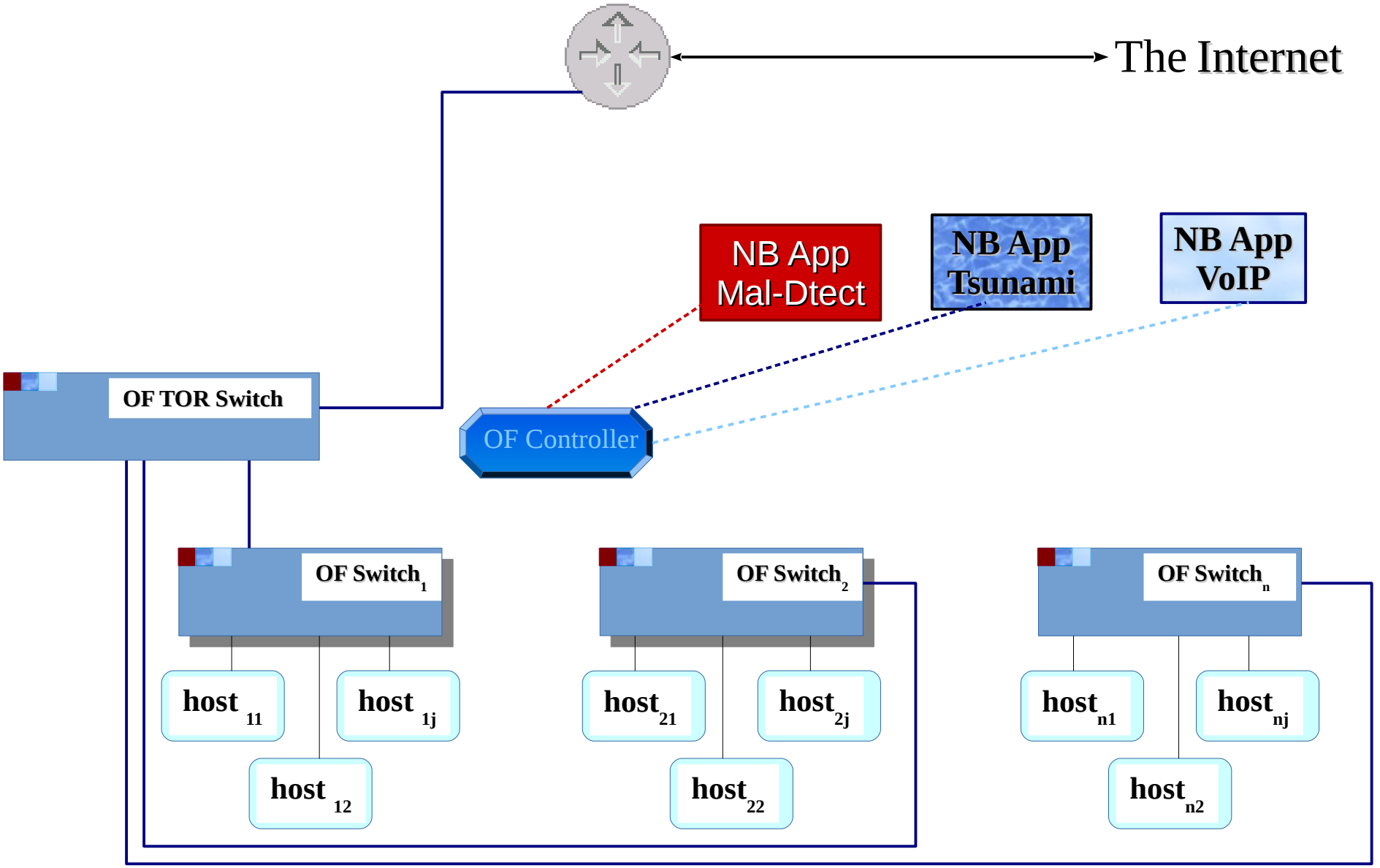
- The Northbound Application (NB App) communicates with the controller
- This combination programs the network infrastructure for a set of traffic engineering functions including network security
- The controlled network infrastructure is optimized for the traffic flows the NB Apps manage.
- Placing 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

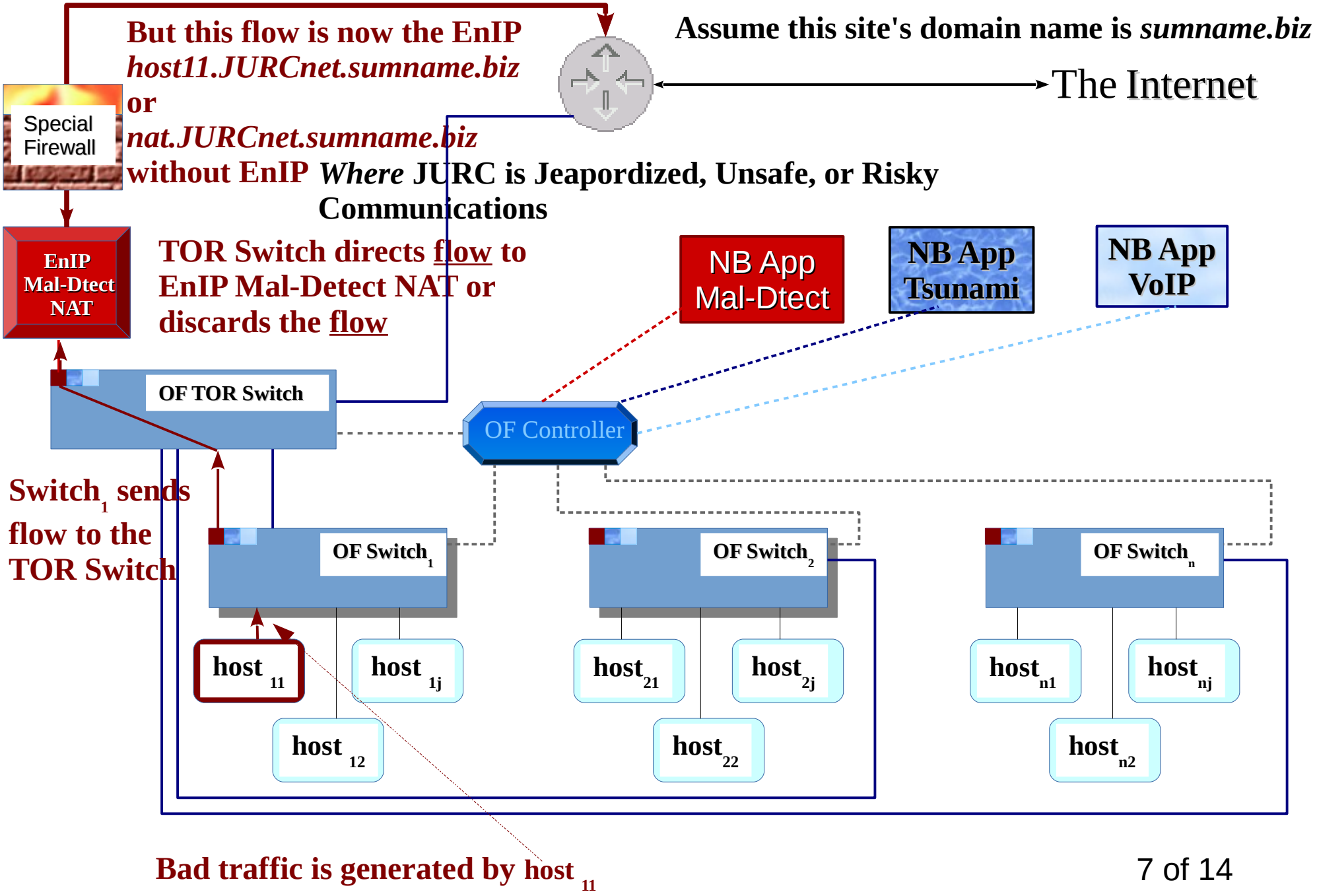
Set up the Northbound OpenFlow Applications



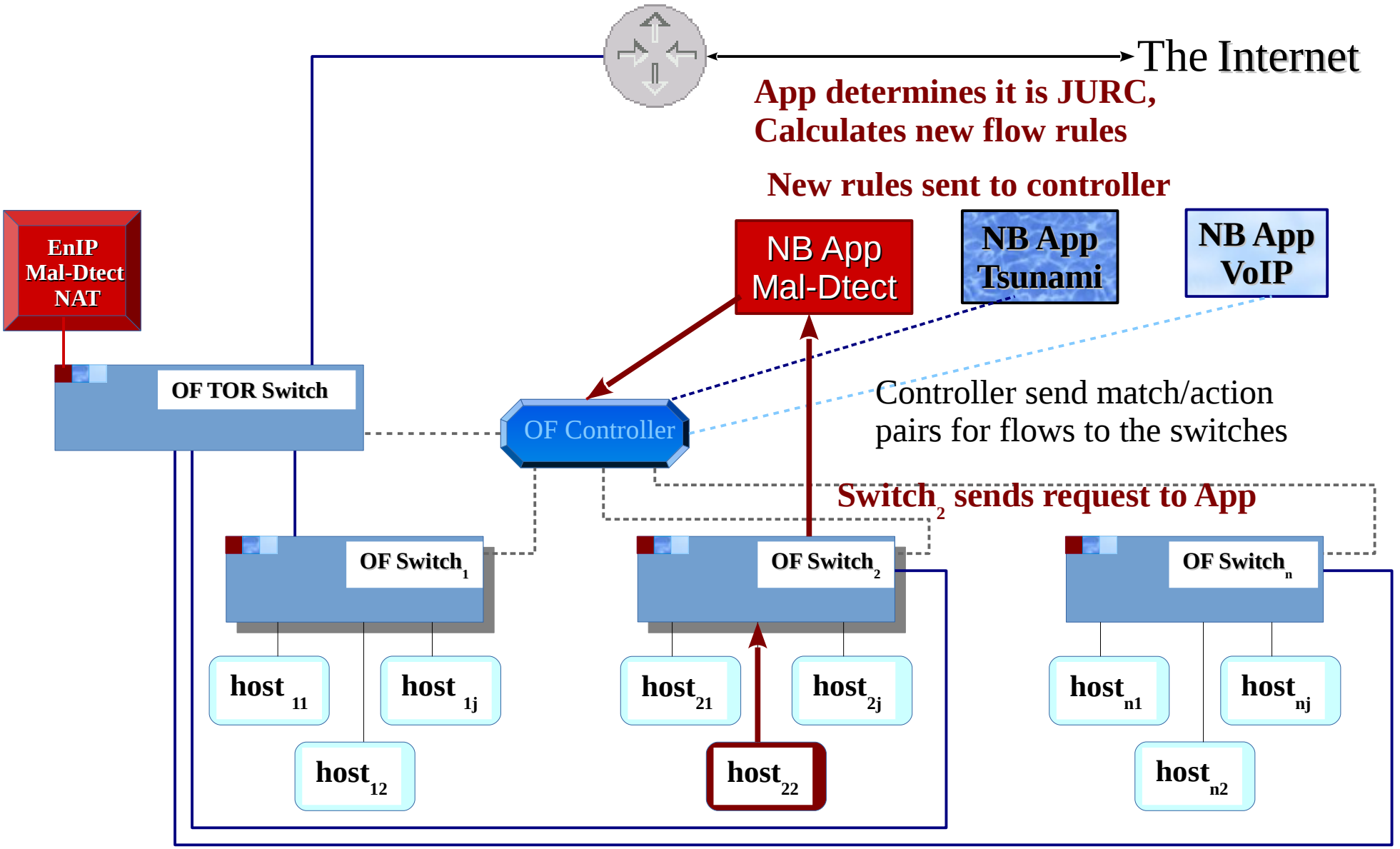
Connect OpenFlow Switch to the Internet



Response to Known Bad Traffic

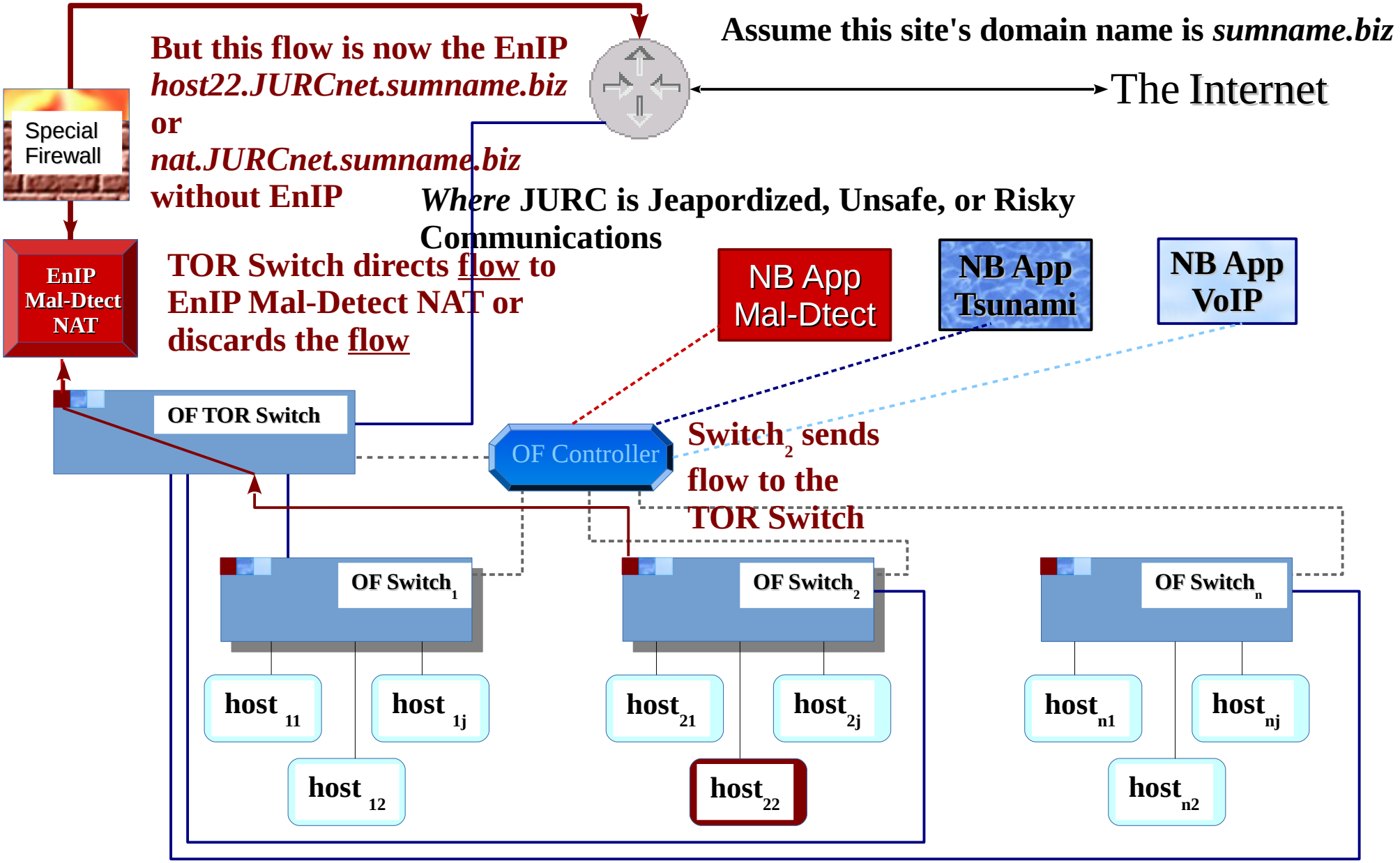


Response to Suspicious Traffic Pt 1

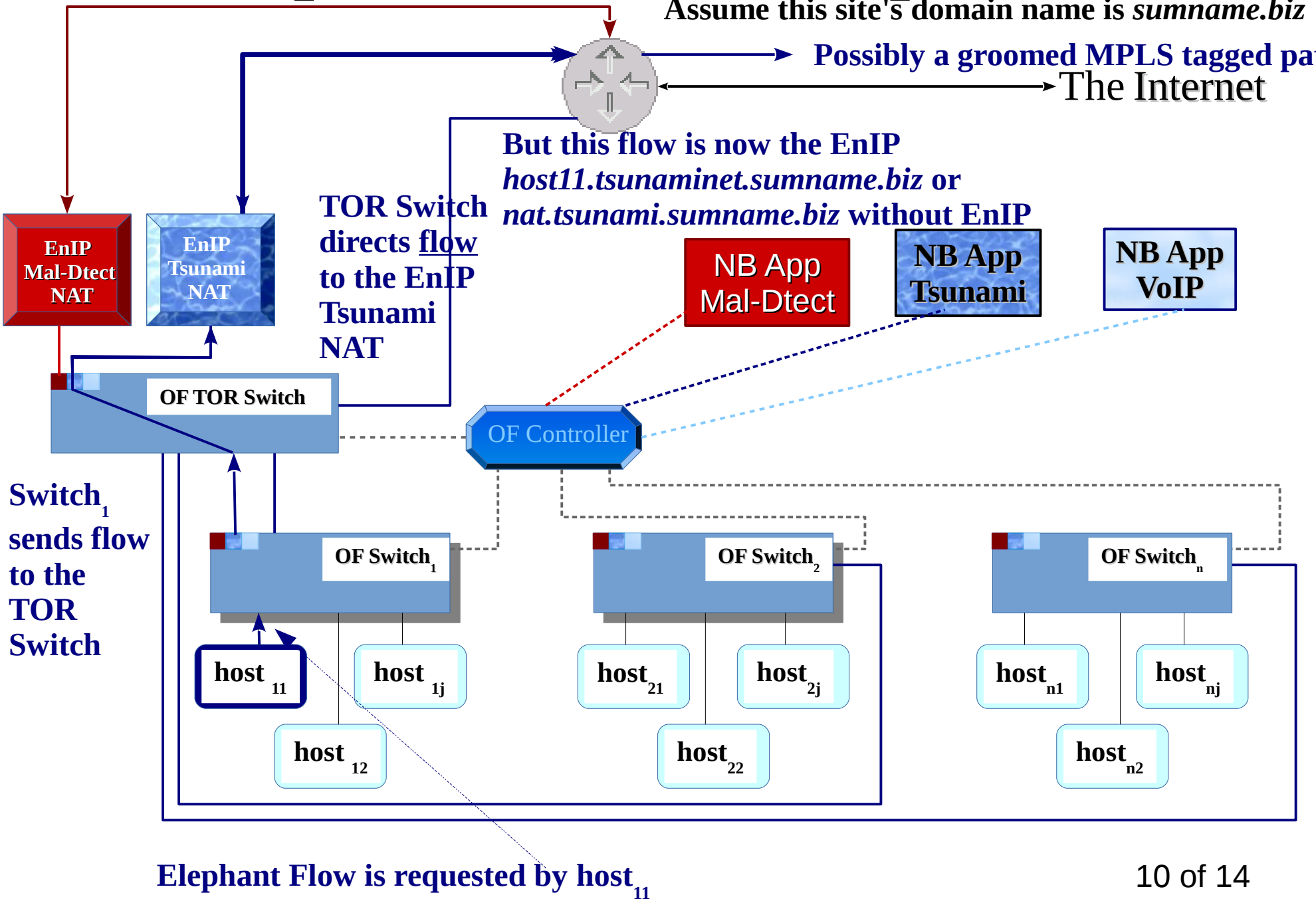


Suspicious traffic is generated by host 22

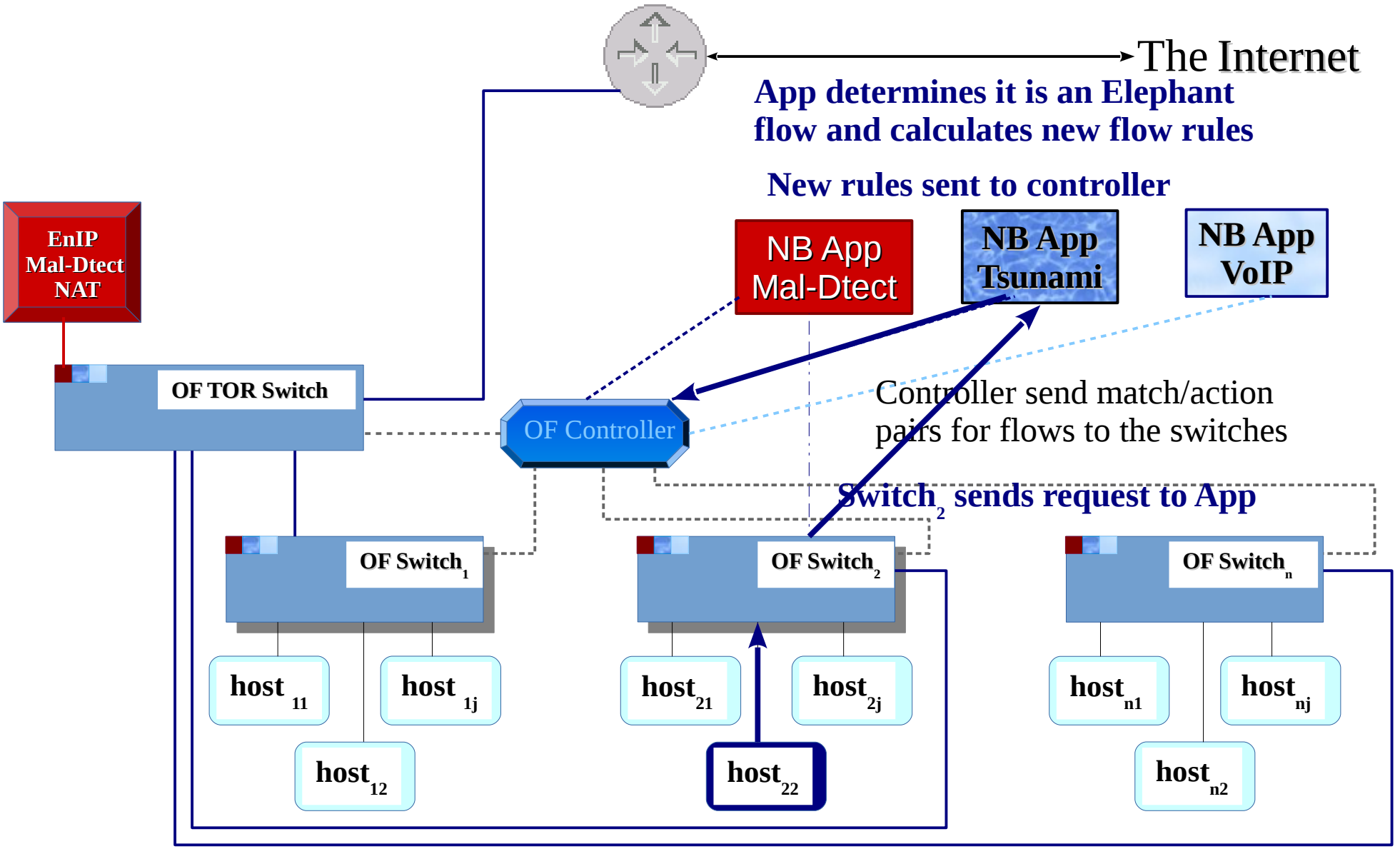
Response to Suspicious Traffic (cont'd)



Response to Known Elephant Flow

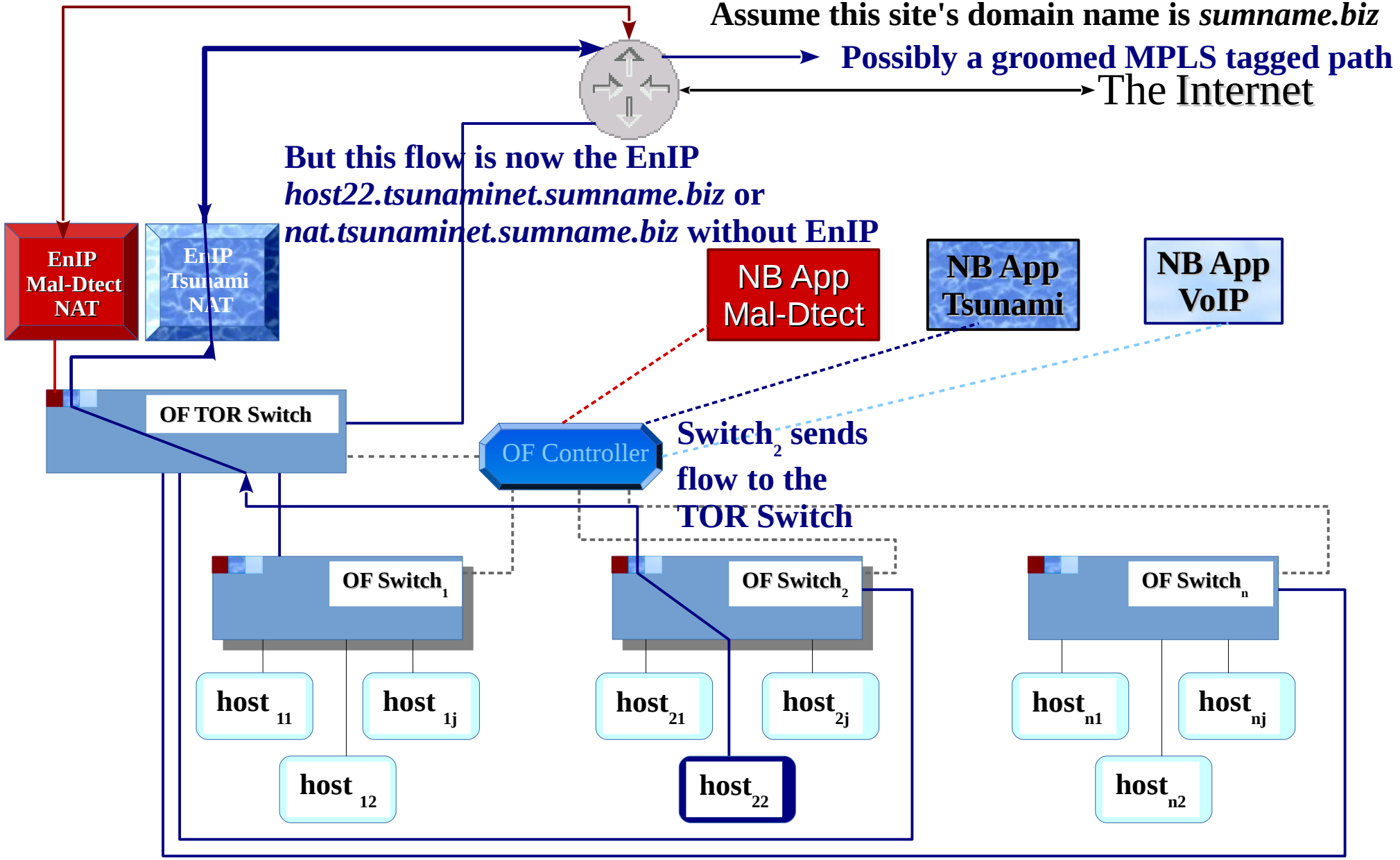


Response to suspected Elephant Flow Pt 1

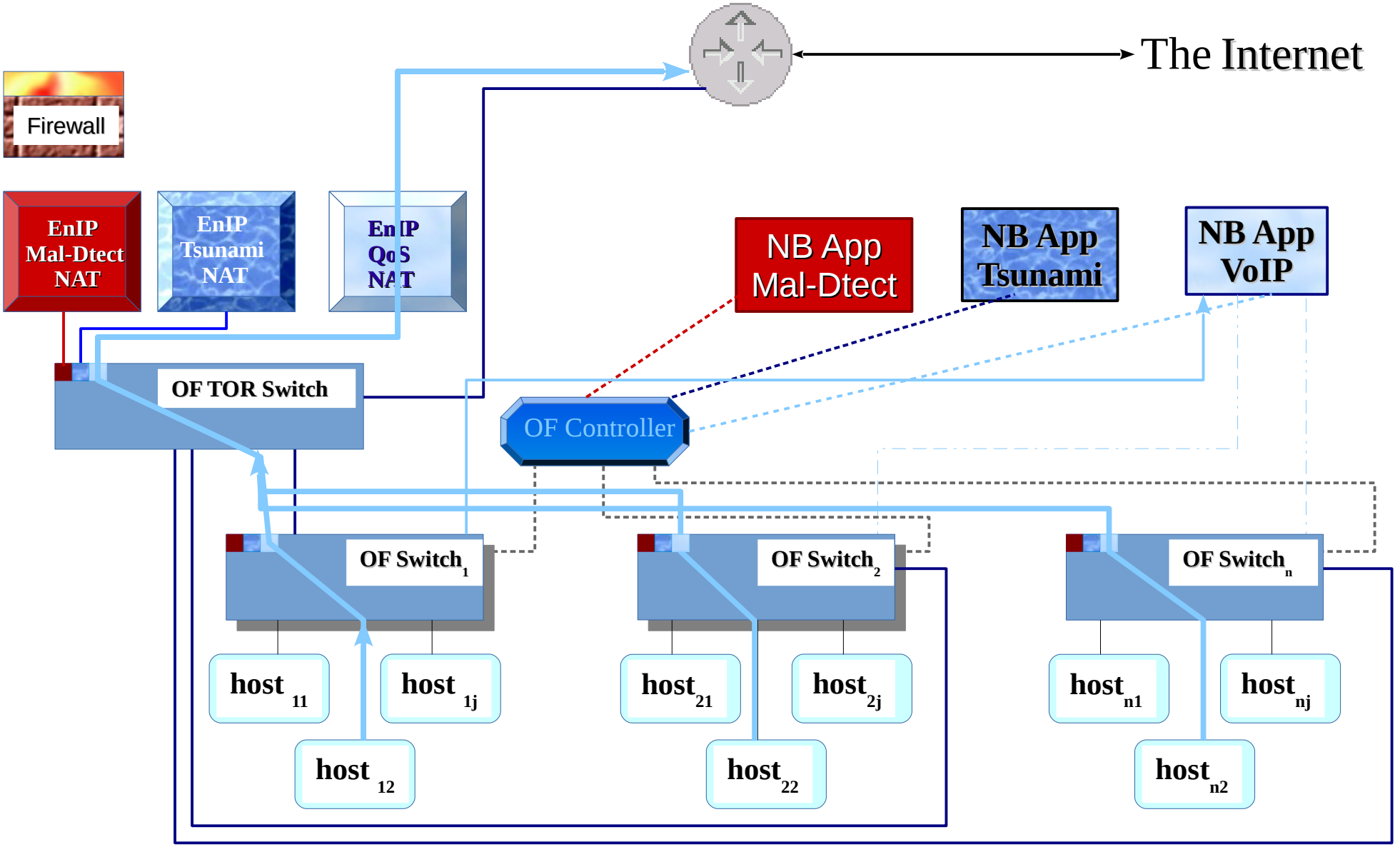


Suspect Elephant Flow is requested by $host_{22}$

Response to suspected Elephant Flow (cont'd)



OpenFlow EnIP Network for VoIP



OpenFlow EnIP Network