Emulytics^{TM} Tool - Firewheel

A virtualized cyber test bed environment

Firewheel is a unique large-scale virtualized test bed designed and implemented at Sandia National Laboratories (SNL). The test bed provides infrastructure for a very large-scale, realistic, and complex network topology and behavior; future development will include capability for running a large number of small experiments concurrently. The virtual network can be used to emulate the functionality of devices in the real world and evaluate their performance under normal and adverse conditions.

High fidelity, large-scale virtualization

The Firewheel test bed environment is able to support over 100,000 virtual machines (VMs) with very high density of VMs per core. For example, approximately 750 VMs with Linux or a light version of Windows 7 can be deployed on a single Dell PowerEdge C6220 rack server with 16 physical cores. The test bed allows for end point heterogeneity; different VM footprints can be deployed to represent different operational environments, such as laptops, desktops, and mobile devices. Additionally, both physical and emulated devices can be supported in the test bed.

Firewheel has a fast setup and boot time, and thus, can be used effectively for very large-scale. It can boot 70,000 VMs with full network convergence in less than an hour. With further infrastructure development, the test bed can be used to run a large number of concurrent experiments at small scale (e.g., 1000 experiments with 10 VMs each). If large-scale test beds are not required, Firewheel can also run on a small cluster with a few nodes or even on a single server.

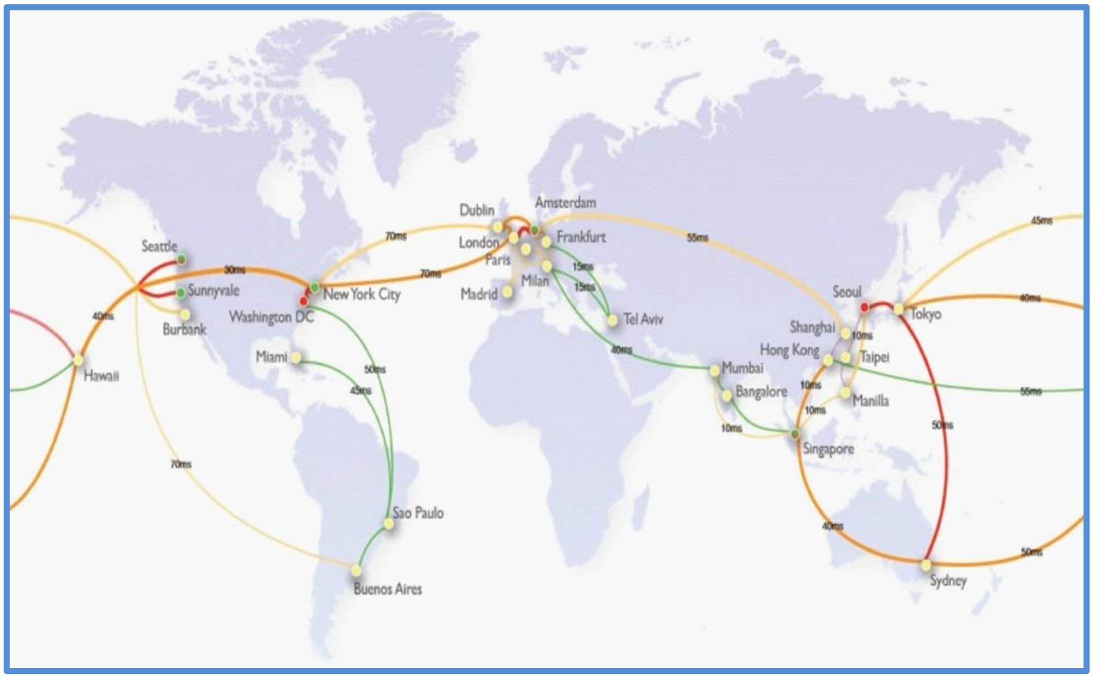

Figure 1. Network topology at autonomous system (AS) level. The color and width of links indicates bandwidth. Real average link time delay is given in milliseconds (ms).

Network emulation

Realistic and complex network topologies are implemented using real world data and network design tools, such as OPNET and CORE. In order to model these topologies, the test bed includes support for:

- Different routing protocols, such as Open Shortest Path First (OSPF) protocol for enterprises and Border Gateway Protocol (BGP) for Internet global routing among autonomous systems (ASes);
- Domain Name System (DNS) and forward DNS zones;
- Network Time Protocol (NTP) server;
- Windows applications including Domain Controller, Exchange, SharePoint;
- Virtualized security devices to describe demilitarized zones (DMZs), or perimeter networks, as part of separate private enterprise networks.

These realistic topologies allow for high-fidelity emulation of Internet-like network conditions, such as route changes, latency, jitter, and packet drop emulation based on traceroute, AS, BGP, and network quality of service (QoS) data acquired from public, academic, and commercial sources. The Firewheel test bed environment provides researchers with (1) the ability to induce different network conditions on both network devices and routes and (2) the ability to induce route changes during the course of the experiment.

Figure 1 provides an example network topology at the AS level. BGP core routers are shown at various cities around the world. A site or enclave's network is comprised of end points and a BGP core router with connected switches and routers. The end points and additional switches and routers can be at city or country level. The network topology also indicates the bandwidth and average time delay of links between core routers.

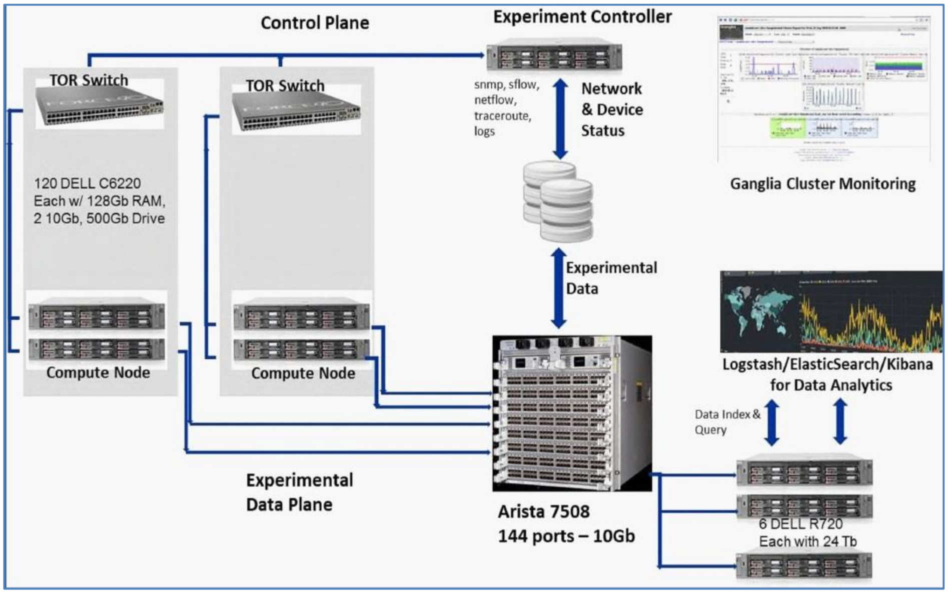

Figure 2. Physical layout of the Firewheel test bed architecture with a control plane for test bed management and an experimental data plane for data collection.

Physical test bed

The physical layout of the Firewheel test bed architecture is described in Figure 2. The test bed consists of the following hardware:

- 100 each Dell PowerEdge C6220 rack servers
- 6 each Dell PowerEdge R720 rack servers
- 1 each Arista Networks 7508 switch with 144 10Gb Ethernet ports
- 3 each Arista networks 7504 Top of Rack (TOR) switches with 48 1Gb Ethernet ports

Across the entire test bed, there is an estimated 200 TB of total storage.

The Firewheel test bed architecture consists of two separate network planes: the control plane and the experimental data. The control plane is used, first, to bootstrap the virtual network and all VMs representing end points and routers; this initialization includes loading any necessary application software onto each end point. The control plane is also used to monitor both the physical hardware cluster and all VMs in the virtual network. The experimental data plane is the virtualization of the experiment's network topology. All communication between devices (simulated, emulated, or system-in-the-loop) in the virtual network occurs on this plane of the test bed.

Test bed management

The control plane is used to monitor state-of-health (SoH) of both the physical cluster and the virtual network (i.e., virtual machines, network links, etc.). Ganglia is used to monitor and display the SoH of the physical servers on the test bed. Additionally, as depicted in Figure 3, a custom virtualization tool was developed to display the test network topology and its SoH.

Data collection

The experimental data plane is used to collect test generated data, such as network communication packets and netflow records. Each experiment can generate a large amount of data, including communication messages and commands, logs, sflow, and netflow records. If there is a very large number of end points (more than ~50,000) on the test bed, it may not be possible to collect all data at all end points. Instead, aggregated data can be collected from different vantage points on the test bed, including at representative and end points and routing devices.

Data analysis

A suite of open-source software including Logstash, ElasticSearch and Kibana is used to organize, index, search, and visualize the collected time series data from each experiment. Custom queries and dashboards can be developed to display results pertinent to each experiment.

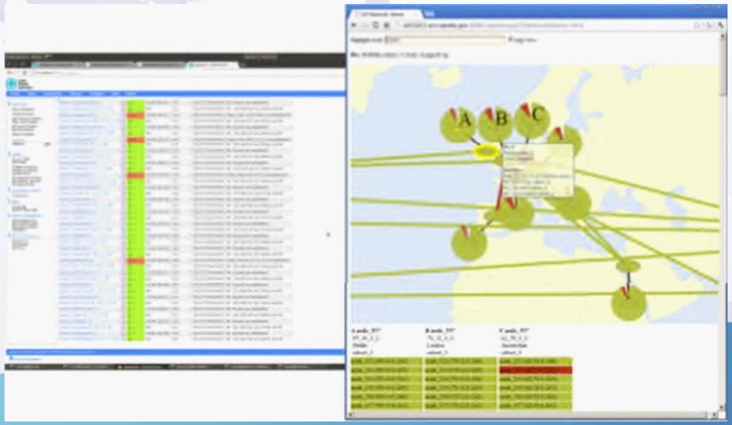

Figure 3. State-of-health (SoH) for the physical servers and all virtual devices in the test bed. Oval nodes represent nodes, radial fans represent the number of VMs connected to a switch, and red indicates that a link or VM is down.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000 SAND2017-1858M

Use Cases

The Firewheel test bed can be employed for several different scenarios, including prototype development, network emulation, malware analysis, critical infrastructure emulation, and system assessment.

Prototype development

The goal of prototype development is the implementation and testing of algorithms for new technologies, such as network protocols or data analytics. Because the Firewheel test bed may allow for many small experiments to be run concurrently, resources can be allocated for a group of twenty (or more) researchers to work simultaneously on the live test bed. Each researcher can generate various network conditions and QoS on different applications. The Firewheel test bed will support the execution of the full lifecycle of research and development (R&D) including prototype development, deployment, testing, evaluation, assessment, and refinement.

Network emulation

The goal of network emulation is the emulation of large-scale enterprise topologies and wide area network (WAN) connectivity with QoS. Because the Firewheel test bed allows for high-fidelity, very large-scale experimentation, researchers are able to leverage topologies and QoS conditions from existing commercial infrastructure. End points can also be scaled to simulate large-scale network traffic. The Firewheel test bed currently supports a 500-router WAN topology based on a large commercial ISP infrastructure backbone at various scales ranging from 5,000 end points to 73,000 end points.

Malware analysis

The goal of malware analysis is to understand malware spread and the rate of infection over a representative network. The Firewheel test bed allows researchers to deploy representative malware samples, such as CodeRed or Blaster, over WAN topologies. This experimentation will support the measurement of rate of spread and infection at different networks, and enable researchers to understand limitations of older worms.

Critical infrastructure emulation

The goal of critical infrastructure emulation is to emulate larger supervisory control and data acquisition (SCADA) systems. Firewheel supports the integration of SCEPTRE, a virtual control system environment developed at SNL, for simulation of all necessary control system components. The Firewheel test bed deploys and manages all SCEPTRE resources and the appropriate switch fabric. An integrated Firewheel and SCEPTRE environment has successfully deployed a 300-bus IEEE test system of remote terminal units (RTUs) and front end processors (FEPs), all backed by a physical-system simulator (Powerworld, in this case). The environment is currently being used to deploy a 6,500-bus system.

System assessment

The goal of system assessment is to characterize the operational envelope for a given software and network. Because the Firewheel test bed allows for rapid experiment deployment, researchers can deploy the application on networks of varying scales and under different resource profiles (i.e., light, medium, and heavy loads) and adverse network conditions. The Firewheel test bed supports the collection of all data from this application load testing. Analytics can be performed in Splunk on large network data (~73,000 end points) that is collected from a variety of sources, including netflow, host logs, VM logs, and traffic captures.

Contact Us

emulytics@sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000 SAND2017-1858M