HOSTING AN IEEE INTERCLOUD TEST NODE
March 2013

THE IEEE INTERCLOUD TESTBED (“the Intercloud Testbed”) is an overlay testbed designed to allow researchers to experiment with cloud computing platforms and services that benefit from distribution across a wide geographic area. All uses of the Testbed should be consistent with this high-level goal.

This “Hosting an IEEE Intercloud Testbed Node” document was directly derived from “Hosting a PlanetLab Node”, PlanetLab Consortium, 2007.

The Intercloud Testbed is designed to support both short-running experiments and continuously-running services. The former includes network measurement experiments that purposely probe the Internet, while the latter may serve an end-user community. In running these experiments and services, we expect researchers to adhere to widely-accepted standards of network etiquette, as well as adhere to the specific behavior defined in a companion document: The Intercloud Testbed Acceptable Use Policy (AUP).

Hosting Site Responsibilities

Hosting a Intercloud Testbed node implies supporting Intercloud Testbed's research goals. In particular, hosting sites are expected to do the following:

- Provide IP connectivity for the node, including a single static IP address and a DNS name (including both forward and reverse lookup).

- Place the nodes outside the local firewall, in a network DMZ. This implies not filtering traffic into and out of Intercloud Testbed nodes. In general, sites should take reasonable steps to isolate their Intercloud Testbed nodes from the rest of their institution's computer systems.

- Allow the Intercloud Testbed operations team to administer the node, including have root access, install and maintain the operating system, and set up research accounts.

- Define a point-of-contact that can be called to re-boot an Intercloud Testbed node.

- Forward complaints from external system administrators to the Intercloud Testbed operations team.

- Enforce the Intercloud Testbed AUP with regard to the actions of local users on any Intercloud Testbed machine, whether hosted locally or at another institution. The Intercloud Testbed community relies on each hosting site to stop unacceptable activity originating at that site.

- System administrators at hosting sites are strongly encouraged to produce and then follow a Technical Contact Guide for more information about what's involved in hosting Intercloud Testbed nodes.

Intercloud Testbed Responsibilities

The Intercloud Testbed operations team will install software on Intercloud Testbed nodes that enforces constraints on application programs, thereby limiting their effect on other network users. These constraints include:

- Limit outgoing network bandwidth. The local system administrator will be allowed to set the total outgoing bandwidth that can be consumed by the Intercloud Testbed nodes they host.

- Filter packets addressed to certain destinations. Our policy is to not filter outgoing packets unless explicitly asked to do so by a network administrator that believes his or her network has been "attacked" from an Intercloud Testbed node.

- Not allow applications to spoof IP addresses, or send well-known bad packets (e.g., "ping of death").

- Limit the rate at which probe packets and other potentially disruptive packets leave the site. The Intercloud Testbed operations team will establish limits that are consistent with Internet norms.

Intercloud Testbed should provide an administrative capability that can be used to set these parameters on local machines. It should allow administrators to inspect packet logs and run an enhanced version of tcpdump that can relate packets to slices, and hence, projects and institutions.

Note that it is likely that individual sites that host Intercloud Testbed nodes will have their own AUPs. Since we expect sites to place their Intercloud Testbed nodes outside their firewall, the "internal behavior" aspects of those AUPs are not likely to be relevant (except as they address bandwidth consumption). However, since administrators are likely to care about whether nodes running on their site exhibit "external behavior" that is contrary to their AUP, our policy is to support site-specific requests for restrictions (e.g., packet filtering) to the extent possible. Should such restrictions be contrary to Intercloud Testbed's stated goal of supporting research into wide-area services, however, it may be the case that the only resolution is to remove the Intercloud Testbed node from that site.

Hosting sites can also expect the Intercloud Testbed operations team to take the following steps to ensure the security and integrity of the software running on each node.

- No users other than the Intercloud Testbed operations team have root access to Intercloud Testbed nodes.

- To reduce the chance of a remote root exploit, all Intercloud Testbed nodes run only a limited set of remotely accessible system services as root. All other standard system services—e.g., FTP, TELNET, and SMTP—are disabled. Services that are enabled on the nodes include SSH (RSA authentication only), HTTP, and finger. For SSH, it should be considered to use OpenSSH v3.7, which is free of any known security vulnerabilities. For HTTP and finger, consider using bare-minimum daemons (both a page of Python code) that respond to all incoming connections the same way: by returning a single file with contact information.

- To reduce the chance of a local root exploit, all nodes should be kept up-to-date with security patches. The operations team should keep track of the latest security patches and update all the nodes. They also should track CERT advisories, ISS security advisories, and security vulnerabilities posted to security mailing lists.

- To further reduce the chance of a local root exploit, remote access to Intercloud Testbed nodes should be done using sandboxed execution environments. These execution environments are chroot'ed and further constrained by also limiting the set of processes, IPC resources, network interfaces, and so on, that can be accessed with a sandboxed execution environment. In summary, once you're placed in a sandbox, the scope of your activities should be limited to that sandbox. Therefore, even if an account is compromised, a hacker still won't have access to root on the machine, and the limitations outlined above will be enforced.

- Monitoring software installed on nodes should provide an audit trail in the event of a security breach.

- To respond to security issues and potential security breaches in a timely manner, report incidents to the Intercloud Testbed operations team.

To reduce the opportunity for unknown users to abuse Intercloud Testbed services, the Intercloud Testbed operations team reserves the right to restrict end-users (clients of services running on Intercloud Testbed) to those affiliated with Intercloud Testbed sites