Prevent idle SSH network drops

Firewalls will often drop idle ssh connections. You (on your client) and/or your server administrator (on your server), can take steps to ensure connections stay alive and thus are not dropped.

IT Security Office's info on this, as of March 11, 2016, for ADOMS

1. Idle timeouts and disconnected sessions

One of the big issues reported to us in the course of Managed Firewall migrations has been session timeouts; users of persistent ssh sessions, persistent Oracle sessiosn, and the Library's Voyager application have experienced untoward application timeout issues.

Since the Managed Firewall infrastructure maintains state tables, it has to do housekeeping and expire state table entries that have been idle. By default, the infrastructure has a state table timeout of 300 seconds, and a session TTL

("time-to-live") of one hour.

To address this issue, we have configured Global Service Objects for ADOM administrators to use, which extend the session TTL to ten hours; more information on using these objects can be found in our ADOM Administrator

documentation:

https: //confluence.cornell.edu/display/itsecdocs/Managed+Firewall+Service

https: //confluence.cornell.edu/display/itsecdocs/Managed+Firewall+Service#ManagedFirewallService-TrafficFilteringIssues

; alternatively, you may always contact us for assistance using these Service Objects or custom-configuring session TTL's yourself (if, for example, you need timeouts longer than ten hours).

IT Security Office's info on this, as of March 2016:

Traffic Filtering Issues

Problem : ssh connections silently disconnect when left idle, yielding a "broken pipe" or similar message

Root Cause: an idle ssh connection, by default, sends no traffic, which allows the connection to time out in the Managed Firewall state table. The state table cannot have a timeout value longer than the default 300 seconds

Solution/Workaround: ssh can be configured, either on the ssh client or ssh server side, to send periodic keepalive packets.

on the client, in the file "ssh_config" in either /etc/ or /etc/ssh, use the lines:

Host *

ServerAliveInterval 300

ServerAliveCountMax 2

on the server, in the file "sshd_config" in either /etc/ or /etc/ssh, use the line:

ClientAliveInterval 300

- Managed Firewall Service#TrafficFilteringIssues

Information from Chemistry IT

- On networks with firewalls, such as at Cornell, an ssh connection will be dropped if it remains idle.
    - A drop can be prevented by configuring the client and/or server to send a “keep alive” packet so the connection is not strictly idle.
    - The idle cut-off time on Cornell's networks is about 5 minutes. Thus, a keep-alive of 4 minutes should suffice.
- In Chemistry IT, we have set all our servers to 4 minutes and that has seemed to work well for our researchers (as of April 2016).
- MacOS clients: No good solution, alas.
    - Chemistry IT is trying to craft a better solution at the network level. Contact us for an updated status report.