

## DNS based ACLs failing

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-07/0013.html>

---

**From:** Dawn ([dawn.m.connelly\\_at\\_usace.army.mil](mailto:dawn.m.connelly_at_usace.army.mil))

**Date:** 07/01/04

Date: 1 Jul 2004 10:17:06 -0700

Starting some time in early June, we started getting reports of the uber annoying "I can't get to xyz webpage". Most of the time, those are PEBCAK errors, but the complaints keep mounting. When I started digging in to it, it looks like they are legit. The users were getting 403'd on webpages that they should have access to. It's cross platform....mickeysoft and sun. So far reports have been for Netscape Enterprise and again, mickeysoft webservers. The one common thread that I'm seeing is that it looks like the Denies happen when the https acl references a DNS query rather than an IP range. So any acl saying \*.gov is good ain't working. But if the class b is there, users are sailing. Reports have been from here in Portland and in Chicago...totally different networks, different sysadmins, different DNS servers. Has anyone else been seeing this recently? I dug through the config file of one of the servers, and everything looks fine. That particular server is also a email bridge head- if DNS were really failing on it, about 3000 people be griping about not getting their SPAM. Any suggestions?