IOWA STATE UNIVERSITY
IT Services Technical Notes
IT

Windows Enterprise Announcement

Sep 27, 2011 – Protect Your Systems from Off-Campus RDP Attacks

As discussed in the September 27 CCSG meeting, a low level distributed attack against RDP (Windows Remote Desktop Protocol) on campus desktops is taking place. As of 11 AM on Sept 26 852 systems have been attacked resulting in over 600,000 failed authentications. ITS recommends that administrators take one or more of the following actions:

- Disable RDP wherever possible
- Firewall RDP to only campus IP space. Group Policy objects have been created to assist with this:
  - ISU RDP [TEST] – Allows only administrative subnets + research park.
  - ISU RDP VPN ONLY [TEST] - VPN subnets only.
- Move RDP to an alternate port: http://support.microsoft.com/kb/306759

.