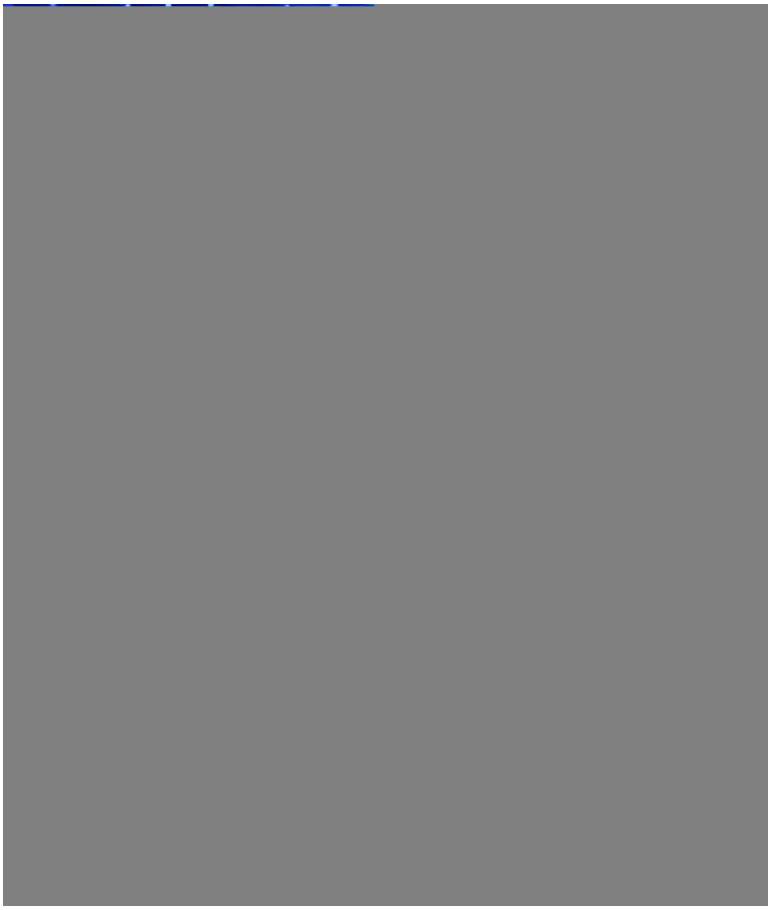
WHITE PAPER

Best Practices *to Secure Your Time Server*

Network security trends continue to evolve in clou Ґ Ç Mшnd

800-207). In part, ZTA refers to the narrowing of network defense perimeters down to individual or small groups of resources. EndRun Technologies has a long history of engineering trustworthy and secure network equipment that is inline with this NIST publication.

Since EndRun Time Servers have a very specialized function - to serve accurate and reliable time, the operating system has been streamlined to remove all unnecessary protocols. This greatly reduces any potential attack surface. Any software that might be connected to a CVE will probably not be present in an EndRun appliance. In addition, all convenience protocols and interfaces like httpd, snmpd, telnetd, sshd and the console port can be disabled. System settings are only modifiable with administrative access (root user).



Following are steps we recommend to secure an EndRun Time Server on a Zero Trust Network. For installations on a public network there should be additional safeguards such as changing User Accounts. These additional safeguards are not described in this paper.

CHANGE DEFAULT PASSWORDS

EndRun Time Servers ship from the factory with two default passwords. The passwords should be changed as soon as possible. There is usually no need for anyone other than the network administrator to log in to the Time Server. Therefore, only one or two persons should know the new passwords.

DISABLE UNNEEDED PROTOCOLS

EndRun Time Servers are shipped from the factory with the following services running. You should disable all the protocols that you do not need, except do NOT disable the Network Time Protocol (NTP).

- NTP (UDP 123)
- TELNET (TCP 23)
- Daytime (TCP / UDP 13)
- Time (TCP / UDP 37)
- SSH (TCP 22)
- SNMP (UDP 161 and 162)
- HTTPS (TCP 443)
- Optional Precision Time Protocol (UDP 319 and UDP 320)

RESTRICT ACCESS

The Time Server should be one of the most secure boxes in your system. Many users may have client access via one of the timing protocols (such as NTP). But the network administrator is the only one who should have direct access. Therefore, direct access should be limited to specific hosts and one or two users.

For the most sensitive situations, you can eliminate all protocols (except NTP) and use the local RS-232 console port to configure and monitor the Time Server. Or, if xexc

` ` F p xc im can r a a

EndRun TECHNOLOGIES
"Smarter Timing Solutions"
Santa Rosa, CA, USA
TEL 1-877-749-3878
FAX 707-573-8619
www.endruntechnologies.com