

netGURUS Security Details

Perimeter security via multi-tiered firewalling

netGURUS' servers are protected with software-based firewalling. These look at source and destination addresses, and source and destination ports. Security administrators handle all aspects of firewall management. Our engineers are familiar with many types of firewall applications, including CheckPoint, ipchains, ipfw, ipfwadm, etc. We are able to modify response packets with masquerade responses to the remote initiator. Our systems are secured using the latest security methods including router access list filtering on inbound carrier feeds and firewalling at the SYN level on internal devices.

Monitoring security systems and processes

All security systems are tested on a monthly basis. We use security scanners such as Nessus, (www.nessus.org), and SAINT, (www.wwdsi.com/saint). Automatic updates are instantly made with the latest exploit/DOS, (Denial of Service), check codes. This provides us with an accurate and detailed report on our systems. Our security team is also subscribed to all the major security mailing lists, including BUGTRAQ from securityfocus.com. These lists provide access to the latest security information, which enables us to patch newly found exploits within hours of their discovery.

Intrusion Detection

We currently use a number of intrusion detection applications such as TRIPWIRE, along with our own proprietary monitoring and logging systems. These systems notify our security response team during scans and potential DOS attacks. We react to these situations immediately, modifying ACLs as needed. In certain cases rules are implemented automatically during detection.

All suspicious activity is logged hardcopy directly to a printing station which is monitored closely. This ensures there is no tampering with conventional softcopy logs.

Anti Virus Measures

Our systems are protected against viruses by extensive built-in access controls. Regular users are unable to access or damage system files.

Offsite Backups

Automated offsite secure storage backups to our mirrored storage arrays in the southern US are conducted through secure encrypted tunnels using SSH with confidential data encryption prior to transit.

Disaster Recovery Procedure

Our disaster and recovery site is currently located in the South Eastern United States. This site is for the sole purpose of emergency fail over. This NOC is capable of handling all traffic in case our eastern operations is interrupted, however we have



taken every precaution necessary to ensure our services will be available under all circumstances.

This site is also set up in a redundant, robust, high availability clustered environment. This allows multiple equipment failures with zero degradation in service. All sites are designed and implemented as exact duplicates to ensure the operating environment remains the same. users are unable to access or damage system files.

Recording and determining access to data

Every employee with access to internal computer interfaces that includes customer data is assigned a unique username, ID number and password. Access to customer data is restricted based on the responsibilities of each employee. Each user is assigned an appropriate access level. Employees are only granted access to information that is essential for them to efficiently perform their job requirements. The actions of each individual on the computer system are recorded and logged by employee ID number.

Printed documents that include sensitive customer information are protected in locked file cabinets. An access control system that uses key fobs restricts access to server rooms and programming areas. Individuals are granted access to these areas only if it is essential for them to effectively perform their responsibilities.

Our practices regarding the protection of customer information are captured in our Privacy Policy. The Privacy Officer is responsible for ensuring the responsible management of all customer information.

Passwords

All passwords must be changed from vendor-supplied defaults upon initial use. To ensure the effectiveness of security parameters, we recommend a combination of uppercase letters, lowercase letters, numbers and symbols for each password. Employee passwords are regularly tested to ensure that they are not easily compromised.

Secure Server Details

We are using Linux-based Apache with 128 bit SSL encryption.

Offsite secure storage is performed at both of our remote NOCs. These backups are done through secure encrypted tunnels using SSH, with confidential data encrypted prior to transit.