

SECURITY



Secure

To protect technology infrastructures from internal and external threats and risks through centralized network risk management, security policy enforcement and remediation techniques.

Why Secure?

Defining and implementing security policies is not an easy task for a network administrator especially if the network is multi-vendor and multi-technology. In addition keeping track of network device configuration changes for any potential security vulnerabilities is a complicated process and requires well experienced IT personnel.

How We Do It

Paritra Security Solutions monitor and enforce security of network devices, either through security profiles or through enabling security functionality in network infrastructure. Paritra Security Solutions provide security auditing functionality to assess network devices for security guidelines such as National Security Agency's (NSA) router/switch and firewall guidelines, or Security Management best practices by ISO 17799 standard. Once a vulnerability is found secure configuration is generated to fix that vulnerability.

Pari Networks Components Used

Dashboard

Monitors security policy compliance charts.

Reports

Generates policy and audit report generation, configuration archival reports and system log reports.

Audit

Conducts capability and network status audits, creates policy and profile groups, defines profiles, schedules policy profile audits and generates remediation actions & configurations.

Configuration

Conducts security feature configuration.

About Us

Pari Networks provides effective and easy to use security risk management solution. We have a patent pending approach for combining network operations, regulatory/corporate compliance, security assessments and remediation actions. This enables simplified administration of networks ensuring secure and regulated business operations for our partners and customers.