



PARITRA PRODUCTS PROVIDE OUTSTANDING VISIBILITY AND COMPLIANCE CAPABILITIES

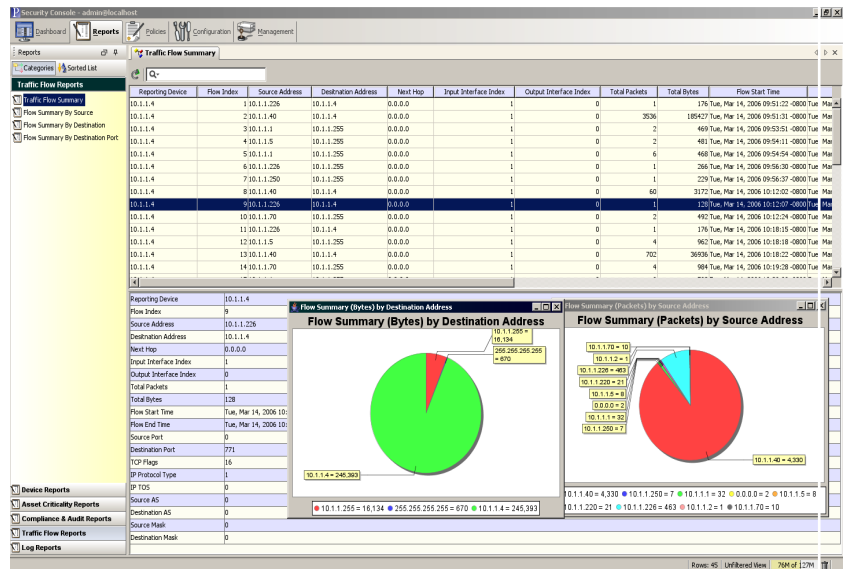
Network administrators are striving to make their network devices comply with government, industry and internal regulations while protecting devices from security threats. To address this, Pari Networks provides a single platform, run either in a centralized or decentralized fashion, to comply with key regulations while providing security and network management, asset prioritization, visibility and mitigation. By providing multiple applications on a single platform, Paritra appliances can provide one-stop solutions for corporate headquarters, small offices and branch offices.

SCOPE OF PARITRA PRODUCTS AND SERVICES

Paritra products support an automated policy framework that helps to manage compliances (SOX, HIPAA, PCI, GLBA, ISO17799), policies, vendor-specific security advisories such as Cisco PSIRTs, and EoX information. Paritra products are available either as appliances (Paritra Appliance Series) or as software bundles (Paritra Software Series) to enable flexible deployment options for SMB and enterprise customers.

Paritra appliances collect and process data and provide centralized security policy and risk management solutions through its applications. Solutions can be broadly categorized into compliances, vulnerability analysis, vulnerability management, security audits and risk mitigation through the generation of automatic configuration updates. The appliance can be installed at the user site or at an MSSP facility.

Pari Wings, enabled in software, are easily distributed data collection points used to gather information about customer network devices which is passed to the Paritra appliance(s) located at the user's facility or MSSP. The collected information can include simple configuration data, performance data, security data, routing information, switching information, and firewall information.



Pari Portal adds easy to use audit capabilities from our servers to implement compliance and security management over the secured internet. This approach doesn't require hardware or software and users only pay to the extent of the audit service usage. The portal provides an area to immediately process the submitted device configurations and produce compliance and security audit reports and is a perfect solution for small to medium size networks.

Group	Paritra Appliance and Pari Wing Features
Security & Compliance Audit	<ul style="list-style-type: none"> Define and enforce security and/or compliance policies Perform vulnerability analysis on network device configuration/capabilities and provide violation reports Generate and deploy network configuration changes required to fix vulnerabilities Monitor for configuration changes or network changes (addition/deletion of network devices), making sure policy compliance is always maintained Customize existing policies and/or create new policies Audit network for vendor security advisories
Reports	<ul style="list-style-type: none"> Collect different data sets like simple configuration related (current device configuration, version information, etc.), performance related (interface status, interface statistics, etc.), security related (access control lists, secure shell, user connectivity sessions, etc.), routing information (routing tables, router VLANs, etc.), switching information, firewall information, syslog and Netflow information Generate service reports (to provide if a given service is enabled or disabled or supported/not supported for a given device)

Group	Paritra Appliance and Pari Wing Features
Management	<ul style="list-style-type: none"> • Provide capability reports (to find out if a given device is not capable of a specific service, whether due to SW or HW) • Provide detailed analysis of End of Life, End of Sale, End of Support for both software and hardware • Provide syslog and netflow data based reports • Ability to combine capability, compliance and end of life reports to generate compliance capability reports (to determine if a given device can ever be compliant to a specific regulation) • Export the reports and graphs into many different formats • Easily find sought information <ul style="list-style-type: none"> • Discover devices using various discovery mechanisms (known devices, seed file, CDP, IP Scanning, SNMP, etc.) • Collect information from devices using both System Credentials (read only credentials for the system to collect data) and User Credentials (individual user credentials for making changes to the device) that can work with various protocols like telnet, ssh, http, https or snmp • Customize syslog data collection from various devices • Create Device and Interface groups for applying policies • Perform distributed data collection • Role based access to the system (Executive, Auditor, Network Admin and Super Admin roles) • Version based configuration archival (for both Running Configuration and Startup Configuration) • Diff utility to view differences between configurations • Label based configuration archival (set up labels to set of device configurations) • Layer 2 topology
Configuration Utilities	<ul style="list-style-type: none"> • Wizard-based configuration applications (walk through steps and generate/deploy configuration) <ul style="list-style-type: none"> - Multi-device configuration - SNMP Configuration - AAA Configuration - RIP Configuration - Firewall Configuraiton - SSH Configuration - RADIUS Server Configuration - Routemaps Configuration - TACACS+ Configuration - NAT Configuration • Template-based configuration applications <ul style="list-style-type: none"> - Security Services (ACL Management, CBAC, IOS-IDS, NAT) - Routing services (Route maps, OSPF, RIP, Static Routing, etc.) - Access Management (Local user management, Terminal Lines, AAA, RADIUS, TACACS) - Global Configuration (CDP, HSRP, Interface configuration, RSH/RCP, TCP, HTTP, SNMPv2, SSH, FTP Client, Banners, Domanin&DNS, TimeZone, SPD, Logging, NTP, DHCP) - Switching services (Switching Interface, VTP, Spanning Tree configuration, UDLD, 802.1x)
Northbound Interface	XML API
Installation & Configuration	Plug and Play hardened security appliance

Corporate Headquarters

Pari Networks
1313 North Milpitas Blvd., Suite 165F
Milpitas, CA 95035
USA
Tel: 408-946-1800
www.parinetworks.com

Asia Pacific Office
Pari Networks
203 Srinivasa Somasikhara
Tilak Nagar
Hyderabad - 500044, AP
India
Tel: + 91 40 27551074