

WHITE PAPER

PROTECT NETWORK DEVICES FROM VULNERABILITIES WITH PARITRA APPLIANCES AND SOFTWARE

Network devices play a pivotal role in managing the communication infrastructure of businesses. However, traditional security management appliances and software do not provide comprehensive tools to protect these network devices from internal and external security threats.

Paritra Suite of products offers applications for wide-ranging vulnerability analysis and security audits. In addition, Paritra solutions can also generate and apply configuration updates to fix the vulnerabilities and protect network devices from known and imminent security threats.

SECURITY CHALLENGE

Computing needs of businesses are growing rapidly. Businesses rely on networked applications to implement and execute complex business processes. This requires increased collaboration and interaction of various organizational elements. Therefore, IT operations have now become 'network centric' to satisfy these requirements.

This increased reliance on networks comes with the burden of efficiently managing the components that make up the network. A typical network landscape includes devices such as routers, switches and firewalls. Unfortunately, security configurations of these components are often incomplete and are prone to internal and external attacks. Moreover, optimal communication service is hampered by the incompatible security configurations. Network device vendors periodically identify vulnerabilities and supply updates or provide a work around until the root-cause of the problem is analyzed. However, updating the network devices is cumbersome and expensive. Attacks on network devices with dissimilar security configurations can cripple the entire company network and cause expensive disruption to business operations. Therefore, there is a strong need for security assessment of networks and network devices.

Traditionally, isolated security assessments are done to identify vulnerabilities. IT and security departments of businesses spend an enormous amount of time and dedicate a number of personnel for this task. Over the years, even these security assessment tasks have become increasingly complex due to the advancement in the network environments. At the same time, security threats are growing and can be fatal. To make things worse, conventional network appliances and software do not provide applications to manage this security dilemma.

A network topology is made up of hundreds of network devices. It is a difficult task to manage and protect all the devices. Even after a security assessment, incorrect prioritization of security configuration management, wrongly identifying the valuable network assets, and miscalculation of the potential downtime can lead to disastrous results. Traditional applications do not offer solutions with prioritization or network asset classification.

After the security assessment and asset prioritization, configurations need to be created for network devices. Generating security configurations requires the help of skilled personnel. Moreover, this is expensive and resources drain for IT departments. Also, the possibility for human errors cannot be discounted.

From network asset management point of view, retiring or continuing with the critical older network devices is a tedious task. Over the years, IT departments can lose track of the security configurations of older devices thereby exposing them to even well-known security threats. When vendors of network devices stop supporting their older devices, implementation of security assessment recommendations to these devices require the time and skill of security administrators.

Companies face security breaches from inside its boundary as well. A disgruntled employee can do detrimental changes to the configuration of network devices. On the other hand, an inexperienced employee can unknowingly make a mistake while configuring network devices. When there are no trails or no security change notifications to the administrators, the mistakes can go undetected. Also, having no ability to see what has changed puts tremendous pressure strain on network administrators. So, we can conclude that a lack of well-developed security audit application that is driven by policies and rules make the security situation highly vulnerable.

SOLUTION: PARITRA APPLIANCES AND SOFTWARE

Paritra suite of products provides centralized security policy and risk management solution. Its products solve issues that are associated with security configuration management of network devices. Apart from handling the reactive tasks of updating the configurations of network devices, Paritra's applications empower customers to perform proactive vulnerability management. As a result, potential security threats are mitigated in a timely manner.

Paritra's easy to use applications help customers to perform vulnerability analysis. Its security assessment can analyze and report the relative vulnerability of the entire network in relation to different network devices that are connected to it. Its unique application architecture helps customers to logically group

network devices during the assessments. So, customers can group devices based on the business priority. Therefore, security assessment and network asset classification/prioritization are synchronized based on customer's business need. This synchronization secures high value network devices and mitigates the risk posed by security threats. In case of a wide-spread security attack, Paritra's applications assist customers to effectively manage threats and run critical business operations without any interruptions. Paritra's solutions also enforce 'integrated security assessment' as opposed to the traditional 'isolated security assessments'.

In addition to assessments, security audits can be done real time with the help of Paritra Suite of products. If vulnerabilities are found, Paritra generates configuration updates to fix the identified vulnerabilities. It also keeps track of old device configurations for future reference thereby serving as a 'configuration management database' for all network devices.

Paritra's advanced policy architecture is unique, where security policies comply with vendor specific security advisories (such as Cisco PSIRTs). So, Paritra helps customers to keep up with the evolution in the network devices by supporting their respective vendor's patch management process.

Paritra's easy to use wizards help network administrators with the configuration of all applications. Also, keeping track of changes to the network device configurations and policies across the network is much easier with its reports. This assists customers to keep track of changes made by the network and security administrators. During security violation, Paritra generates e-mail notifications to inform a company's security organization about the breach. These notifications help customers to take swift action to mitigate the violation.

Paritra series:

- Makes security configuration management of network devices easier and controllable
- Eases the administrator's job of configuring, monitoring and managing network devices easier and efficient
- Protects an organization's network and valuable IT assets from known and imminent threats
- Helps to enforce security policies and verify vendor specific security conformance
- Eliminates human errors and assists in avoiding intentional breaches
- Reduces the Total Cost of Ownership in maintaining and retiring network devices

CONCLUSIONS

Networked applications have produced significant gain for businesses through productivity improvements. But, network devices are one of the important agents that make 'networked applications' possible. Paritra suite of products help organizations to protect its network devices, thereby helping to protect its entire network and networked applications.



Corporate Headquarters

Pari Networks
1313 North Milpitas Blvd., Suite 165F
Milpitas, CA 95035
USA
Tel: (408) 946 1800

Asia Pacific Office

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

Pari Networks is head quartered in Milpitas, California, with an Asia Pacific office based in Hyderabad, India.