Tufin Closes the Application Gap in Complex Firewall Management with SecureApp

Event

In September 2012, Tufin Technologies released a new product, SecureApp, intended to help enterprise firewall administrators address one of their greatest challenges – keeping rules that secure enterprise application connectivity current and accurate in the face of rapidly escalating rates of application changes. The new product provides a user interface that can be used to quickly and easily define and maintain application connectivity policies. It works with the balance of the Tufin firewall management solution to automate workflow and configuration changes to managed firewalls based on application additions, changes, or deletions. SecureApp eradicates common process barriers and paves the path toward higher levels of efficiency and accuracy for the interdependent processes of network, applications and security operations to improve performance and assure integrity and compliance across the entire managed infrastructure.

Background and Context

As IT has grown in complexity, the challenges of network management have grown as well. Connections have multiplied as businesses have become increasingly interconnected. Automation has become a necessity to maintaining network reliability.

As applications have grown to dominate IT focus, they have added to the challenges of network management. Networking has become an integral aspect of the modern application, with Application Delivery Controllers (ADCs) assuring high availability and performance under demanding conditions, WAN Optimization Controllers (WOCs) providing acceleration for distributed applications and client-side connections, traffic QoS policies created to prioritize application delivery and performance, and more. Developers and application operations managers have grown in their awareness of these critical aspects of application delivery – but there is one area of application-oriented network management that remains too often overlooked.

As applications have grown to dominate IT focus, operations managers have grown in their awareness, but impact to network security systems is still often overlooked

That aspect is the impact of network security systems. In complex networks, firewall rule sets have become so intricate and involved as to pose high risk when modified. The risk is not only to business-critical availability and performance; changes can directly expose sensitive systems to compromise. Often, permissions may be added but never withdrawn or curtailed, even after their need has long disappeared, for fear of disrupting essential connectivity – which exposes organizations to further risk.

The problem is compounded by the added demands complex applications place on networking. Application developers and architects may have a clear understanding of the many moving parts of a complex application – but this understanding is not always communicated consistently to security teams. Network operations may become directly involved in assuring application delivery and performance, through the deployment of ADCs, WOCs or other application-optimized networking technologies, but security systems are not always seen as critical application dependencies. And yet, security systems can have a devastating impact on application availability and performance if not managed on a par

with other application networking demands. As network security systems have grown in their own application awareness, increasingly able to directly control and enforce policy on application behavior and user interaction, they have a more direct impact on applications than ever before. So-called "next-generation" firewalls, which focus on the application layer specifically, are a great example here.

When changes to network security systems must be made to accommodate applications, organizations must recognize that risks must be analyzed thoroughly and consistently, with policy management guided through the cooperation of application managers, network operations and security professionals alike. The demand for this consistency can only be expected to grow, as applications continue to expand and changes accelerate to meet highly dynamic requirements.

The Tufin Approach: SecureApp

Tufin Technologies focuses exclusively on solutions that support large-scale, enterprise-class management of firewalls. Its flagship product, SecureTrack, has many years in the market as a proven multi-vendor solution for firewall operations management. In late 2009, Tufin expanded its core offering with an extensive set of configuration management and workflow automation capabilities via the SecureChange product. The resulting solution put network security managers in position to be much more accurate and efficient in managing firewall and router policies and rulesets, improving infrastructure integrity, compliance, and resilience in the process.

These were valuable accomplishments, but Tufin's vision did not end there. Tufin recognized that the focus of all infrastructure operations was turning increasingly towards (and was increasingly being driven by) applications. Tufin made initial moves to support this trend by becoming one of the first (Tufin claims *the* first) independent firewall operations management solutions to add support for next-generation firewalls, in this case for products offered by Palo Alto Networks, in early 2011. The longer-term goal has been to elevate firewall rules management to become truly application oriented and to connect firewall operations into application-based lifecycles. This is where Tufin's SecureApp solution comes into play.

SecureApp acts as an application-oriented front end to the rest of the Tufin solution, allowing network security administrators to collaborate with application owners, in a language that is mutually understood, to define and maintain application connectivity policies. The connectivity requirements for each application are defined in terms of source, destination, and service/protocol. These definitions can be constructed from the ground up, imported from an external source, or learned from an automated examination of existing rulesets. Application connectivity policy adds, deletes, or changes can all be made from an intuitive graphical interface. Each connectivity definition is automatically tested to see if it is currently supported by existing rules or if a change will be necessary to put it into effect. In the latter case, work tickets can be raised from, and are automatically pre-populated directly within, SecureApp.

SecureApp acts as an application-oriented front end to the rest of the Tufin solution..to define and maintain application connectivity policies

The real power of SecureApp lies in the supporting/enabling capabilities of the rest of the Tufin solution. The core SecureTrack platform automatically checks status of connectivity policies as they are defined in SecureApp. Whenever a work ticket is raised in order to instantiate, update, or decommission connectivity for an application via SecureApp, that ticket enters the workflow and automated provisioning engine within SecureChange. User roles and access definitions are shared across the components, so that identity is retained and associated with actions, which are logged throughout the process for auditing purposes.

Potential Impact

The SecureApp approach has a number of direct, positive influences on the flow, efficiency, and effectiveness of IT operations across applications, networking, and security:

- **Applications development and operations:** Firewall rules have historically been seen as a significant barrier to progress among application development and operations (DevOps) teams. The reasons behind this are practices among firewall administrators that are often foreign to applications teams and manual processes were that much slower than anyone would prefer. SecureApp represents a means to break down barriers of misunderstanding as well as efficiency, via facilitated collaboration and automated workflows. This will be a distinct improvement for DevOps teams that seek to streamline deployment of new and updated applications.
- **Networking operations**: For network operators, firewalls are perceived to be a potential point of failure in the quest to optimize and assure highly available, high performance delivery of applications. By using SecureApp to improve the accuracy of firewall rules definitions, the potential for service interruptions due to accidental misconfiguration will decline. Further, SecureApp's capability for linking rules more overtly to specific applications will aid in cross-team troubleshooting workflows, where any and all changes often need to be understood while trying to track down difficult performance problems.
- **Security operations**: Once application connectivity requirements are defined in SecureApp, security teams have the opportunity to review proposed changes with a clear understanding of connectivity requirements, supplemented by Tufin's capability for analyzing change risks to security policy before changes are put into place. This gives security teams an informed view of proposed network changes to accommodate applications, and adds to deeper and more accurate insight through a more complete picture of the overall security posture. Further, the facilitated workflows represented by the combination of SecureApp and SecureChange will allow firewall administrators to be more responsive to change requests raised by DevOps and IT ops, and more likely to get those changes right the first time, further reducing effective turnaround time.

On a broader basis, across the IT organization, the SecureApp approach can assist organizations in maintaining high levels of integrity and compliance. Since many regulatory obligations focus on data and/or the applications that deliver and operate on that data, providing an application-oriented approach to firewall rules management simplifies and clarifies compliance practices as well as compliance auditing. For example, Requirement 1 of the PCI Data Security Standard describes specific procedures to assure firewall configuration, while Requirement 6 speaks to specific aspects of application security, including the need to mitigate application vulnerabilities. Tufin SecureApp will help organizations address multiple aspects of these requirements specific to firewall, network and application configuration, improving efficiencies and reducing compliance costs.

The SecureApp approach can assist organizations in maintaining high levels of integrity and compliance.

By defining processes for making changes that systematically incorporate input from applications, network and security teams, a broad range of risks can be reduced or eliminated. Risks to network/application connectivity and performance can be reduced by properly interpreting application connectivity requirements into effective firewall policies and rules. And risks of exposures or violations of security policy or required regulatory compliance can be minimized while optimizing the investment of time and expertise on the part of security professionals.

EMA Perspective

Applications have become such a dominant aspect of IT functionality that the makeup of their many moving parts may be better described as a service architecture. As such, they are comprised of many components – compute, storage, networking and software – not least of which are those designed to protect businesses against application abuse, regardless whether from external attack, insider manipulation, or other threats.

By recognizing the integral role that network security systems such as firewalls play in assuring not only application protection but also performance and availability, Tufin has defined a new market opportunity in end-to-end application management. The company's SecureApp extension of its coherent and optimized approach to complex firewall management provides much needed closure to a gap in comprehensive application management that far too often goes neglected, yet one that can have a substantial impact on the business if not managed on a par with other aspects of business-critical applications.