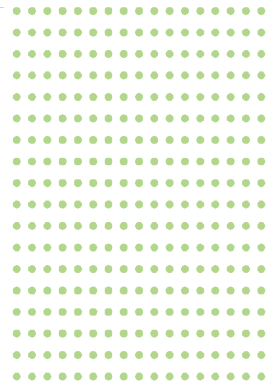


Automatic Firewall Policy Generation

An innovative approach to firewall
deployment that maximizes security
while ensuring business continuity

June 2009

tufin



www.tufin.com

Benelux Sales

T. +31.641.789.667
beneluxsales@tufin.com

Central European Sales

T. +49.89.99.216.441
centeusales@tufin.com

Italy Sales

T. +39.06.43.40.90.17
itasales@tufin.com

UK Sales

T. +44.780.230.4500
uksales@tufin.com

US Sales

T. +1.877.270.7711
sales@tufin.com

International Headquarters

5 Shoham St. Ramat Gan 52521 Israel
T. +972.3.612.8118 info@tufin.com

Table of Contents

The Challenge: Securing More Network Segments – without Service Interruptions	3
The Solution: Automatic Policy Generation	3
How It Works	4
Permissive Rule Analysis Technology	5
Optimizing Existing Firewalls	6
Supporting Regulatory Compliance	6
Conclusion.....	7
Trademarks	8

The Challenge: Securing More Network Segments – without Service Interruptions

Network security teams are frequently challenged by the requirement to secure unrestricted network segments without disruption to critical business services. Some common requests include:

- Securing sensitive internal network segments such as finance and HR
- Securing the connection between branch offices or companies that have merged
- Tightening overly permissive firewall policies.

But as every security professional knows, installing a firewall on an active, currently unsecured network segment is easier said than done. Through labor-intensive manual log inspection, administrators try to identify legitimate business traffic and create a rule set that will meet both security and business objectives.

Given the complexity of network traffic today, this process is not only tedious and inefficient – it is also not very effective. As a result, organizations invest a great deal of resources responding to service interruptions. Today, the only alternative is deployment of an overly permissive firewall policy that does its job more in name than in deed. So in many cases, organizations opt to leave certain segments unsecured rather than risk downtime to crucial business services.

Network security teams need a better way to create new firewall policies and tighten up permissive ones that is both accurate and cost-effective.

The Solution: Automatic Policy Generation

Tufin SecureTrack™ introduces a new approach to firewall deployment called Automatic Policy Generation™ (APG). With APG, managers can automatically generate a new, robust firewall policy based on a thorough analysis of:

- Current network traffic
- Compliance with organizational and regulatory policies
- Alignment with industry best practices

The resulting firewall rule base ensures that business-critical traffic is flowing normally, yet meets corporate and regulatory security standards. APG creates a rule base that is not too permissive, is optimized for high performance and organized for easy management and maintenance.

Fast and efficient, APG processes thousands of logs to create a new rule base within minutes. By repeating the process several times and adjusting a variety of parameters, firewall managers can achieve and deploy a highly optimized firewall policy in hours, rather than in weeks or months.

APG also provides security professionals with a powerful new tool for tightening existing firewalls, re-building complex, heavy rule sets, and analyzing the rule bases of firewalls inherited from other organizations, for example, following M&A.

How it Works

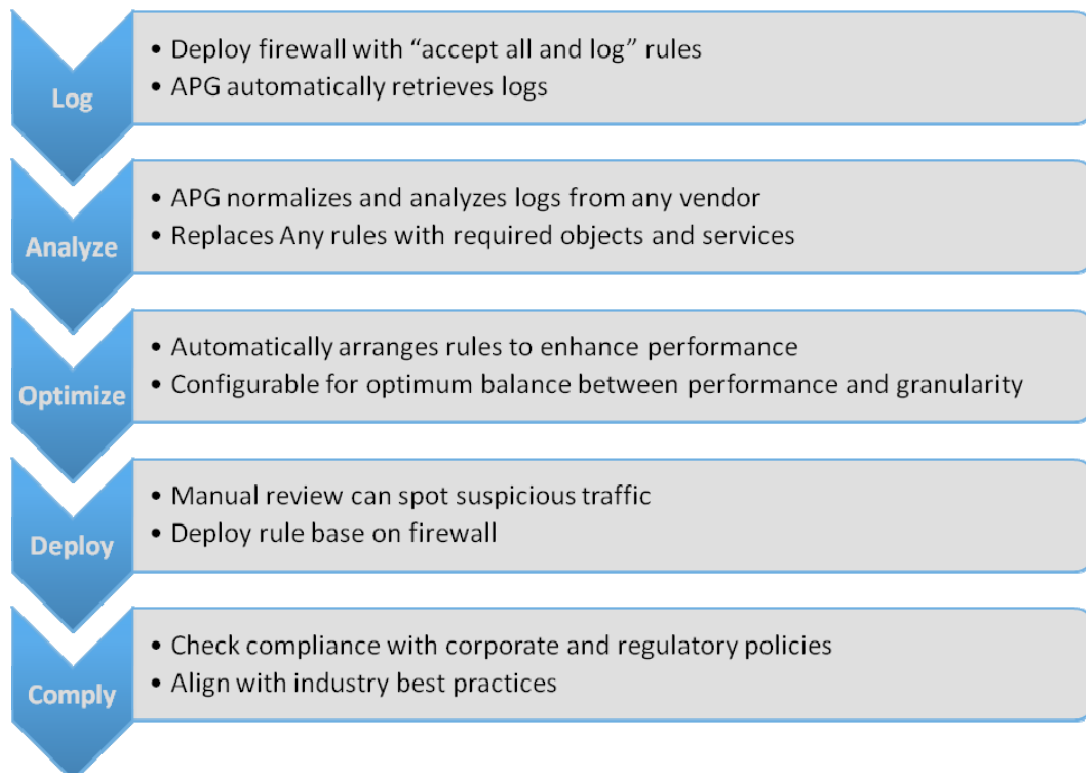
Since APG analyzes network traffic, the first step is to deploy a permissive firewall in the designated location with an “accept all and log” rule. The firewall should collect traffic logs for enough time to capture normal network usage behavior – generally a couple of weeks.

APG then retrieves and normalizes the logs. Using patent-pending Permissive Rule Analysis™ technology, APG analyzes “accept” logs and creates a map of required network connectivity. The network traffic that users need is defined as allowed, while all other traffic is blocked. Rules are refined until they are as specific and accurate as possible, replacing “Any” rules in the original policy with actual network addresses and services.

Within a matter of hours, APG can process weeks or months of log data – from any of the leading firewall vendors - and create an effective new rule based derived from network traffic. To optimize the rule base for faster performance, APG orders rules according to usage, placing the most-used rules on top and the least-used rules on the bottom.

Once automatic policy generation is complete, firewall managers can add unusual scenarios, such as disaster recovery, that may not have been sampled. A careful review of the new traffic-based rule base may also reveal malicious traffic such as a port scan, (even if it runs slowly over several days), a conflicker virus or a generic botnet.

Finally, to ensure that the new rule base is not just accurate but also compliant, SecureTrack can be used to check alignment with corporate and regulatory security policies, as well as industry best practices.



Permissive Rule Analysis Technology

APG is powered by Tufin's patent-pending Permissive Rule Analysis technology, which proactively tightens the security posture of a firewall by rewriting rules that grant too much access. Some common examples of overly permissive rules include:

Source	Destination	Service
WebServers	AppServers	ANY
When the Service field contains ANY between two groups of servers		

Source	Destination	Service
Boston_Office	Net_10.0.0.0	ANY
When the Boston field office contains access to the entire internal network over ANY protocol		

Source	Destination	Service
Net_10.0.0.0	Net_DMZ	TCP:>1024
When the internal network has access to the DMZ on too many ports		

Usually, these types of permissive rules are put into place in order to avoid interruptions to critical business services. The alternative is to define restrictive rules, and then race to respond quickly when users open support calls to complain about broken services. This is not really a viable option for overextended IT organizations.

APG takes exactly the opposite approach. By analyzing traffic logs, APG builds a rule base from the bottom up, allowing precisely the object/service pairs that are in actual business use. APG can even improve rules where all of the objects are used. For example:

Source	Destination	Service	Action
A	X	HTTP	Accept
B	Y		

In this rule, all objects are used, so none can be deleted. However, if A normally only talks to X and B only talks to Y, then the rule can be re-written:

Source	Destination	Service	Action
A	X	HTTP	Accept
B	Y	HTTP	Accept

By splitting up the original rule into multiple, finer ones, security is tightened. APG then groups services and hosts together according to the number of hits per rule, in order to build a fast and efficient rule-base.

APG compresses months of manual analysis and configuration into a day of work. At one data center, APG processed 8.2 Million logs in under 3 minutes.

Optimizing Existing Firewalls

APG is also a powerful tool for tightening security and improving efficiency on protected network segments. By analyzing current traffic logs, APG can identify the permissive rules on any firewall and provide alternatives that are more accurate and secure. APG can be run on an entire firewall rule base, or on a specific section.

For SecureTrack users, APG goes beyond Usage Analysis reports that enable firewall managers to cleanup unused rules and unused objects. APG identifies unused connectivity between specific rules and objects, and automatically generates more specific rules to close those gaps.

Supporting Regulatory Compliance

Eliminating permissive rules and restricting the network to explicitly permit only required traffic is becoming an accepted part of industry regulations. For example, the PCI-DSS audit includes the following:

- **1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business.
- **1.1.5.b** Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.
- **1.1.6.b** Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.
- **1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.
- **1.2.1.b** Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.

APG, in combination with SecureTrack's PCI audit report which provides the required documentation, help organizations to meet these requirements efficiently.

Conclusion

Security professionals need a new approach to firewall deployment that provides both security and business continuity. The current approach produces unsatisfactory results – either security is tight and legitimate users are negatively affected, or the firewall is permissive, and unwanted traffic can get through.

Tufin's Automatic Policy Generator (APG) introduces a new way of creating firewall policies for existing network segments based on a thorough analysis of network traffic. The resulting rule set is accurate and highly optimized for superior performance. The process is extremely rapid, reducing months of painstaking analysis to hours.

In combination with SecureTrack's policy analysis and auditing capabilities, APG provides an end-to-end solution for deploying firewalls that are secure, accurate, efficient and compliant with corporate and regulatory standards.

APG is also a robust tool that enables firewall professionals to tighten security on any firewall, replace old and inefficient firewall rule bases, and migrate to new products. With patent-pending Permissive Rule Analysis technology, APG breaks down wide rules until they accurately and exclusively represent actual traffic requirements. Combined with powerful usage-based rule optimization, Permissive Rule Analysis takes any firewall rule base to a new level of security and performance.

Trademarks

Tufin, SecureTrack, Automatic Policy Generator, SecureChange, and the Tufin logo are trademarks of Tufin Software Technologies Ltd.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.