tufin

SecureTrack™

Securing Network Segments and Optimizing Permissive Rules with the Automatic Policy Generator

www.tufin.com

tufin

Table of Contents

The Challenge: Avoiding and Eliminating Permissive Security Policies

Network security teams are often asked to secure unrestricted network segments without disrupting 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

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 base or ACL[1] 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, and organizations end up responding to a lot of 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™ offers a unique approach to firewall deployment called Automatic Policy Generation™ (APG). With APG, you can optimize an existing policy or automatically generate a new one 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 traffic logs to create a new rule base in no time. By adjusting the APG recommendations interactively, you can achieve and deploy a highly optimized firewall policy in hours, rather than in weeks or months.
Similarly, APG can be run on existing firewall policies – or just specific policy rules – to safely reduce permissive rules without jeopardizing your organizations' business continuity.

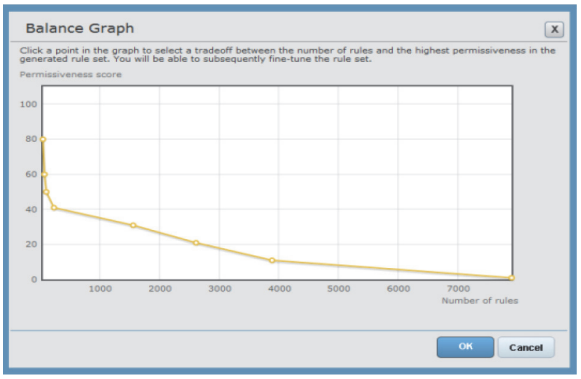
Using APG to Secure a New Segment

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

[1] Automatic Policy Generator supports a wide variety of vendors and platforms. In this whitepaper, we use the term firewall policy or rule base interchangeably with the Cisco term Firewall Access Control List (ACL).

Automatic Firewall Policy Generation 3/7connectivity. 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.

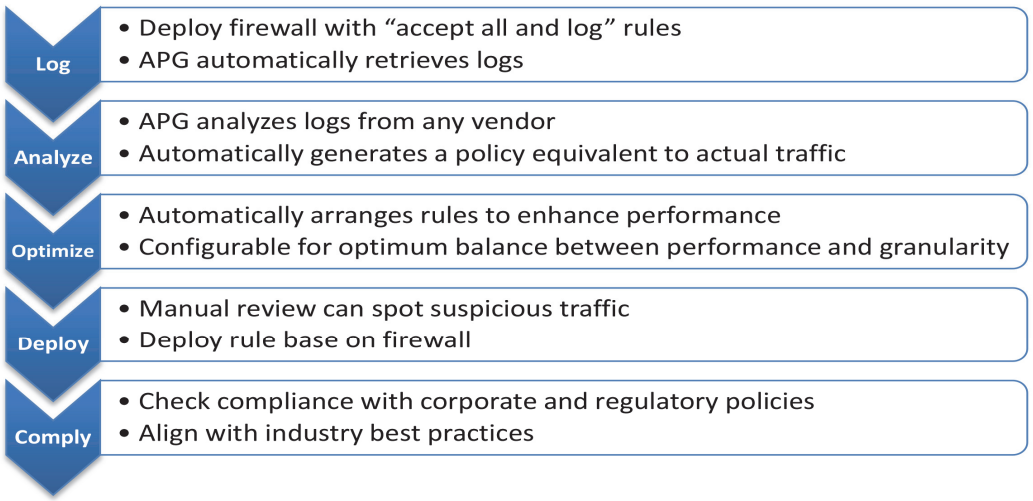
Since there is a trade-off between the degree of permissiveness, and the size of the rule base, APG allows you to interactively determine how granular you want the rule base to be.



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 base 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.

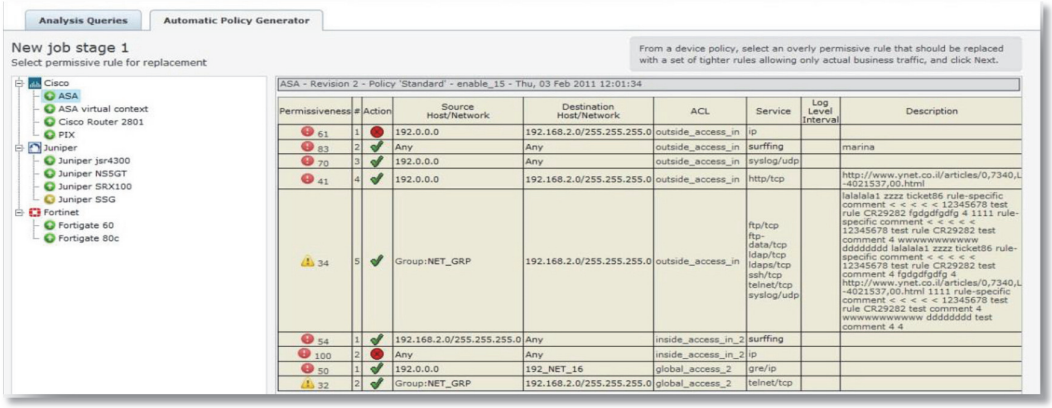
Once automatic policy generation is complete, you can add unusual scenarios, such as disaster recovery, that may not have been sampled. A careful review of the new traffic-based rule base may also reveal malicious traffic such as a port scan, (even if it runs slowly over several days), a conflicker virus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



Using APG to Optimize Existing Firewalls

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



To help you indentify where there is room for improvement, APG reviews the policy on a specified device and assigns each rule a permissiveness score. If you'd like a recommendation on how to optimize a poorly-rated rule, you can set up a log collection task so that APG can analyze actual traffic and propose a new set of specific, less permissive rules.

After the collection and analyses are completed, APG proposes an alternative to the permissive rule, along with the scores for the new rules. Since there is a tradeoff between the number of rules, and the degree of permissiveness, you can use the interactive graph to determine how many rules are created. Afterwards, using an interactive tree view of the generated rulebase, you can fine-tune the results to your satisfaction.

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.

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 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.

1.1.6 Requirement to review firewall and router rule sets at least every six months

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

APG, in combination with SecureTrack's PCI audit report which provides the required documentation, helps 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) is an advanced 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. Without APG, it is virtually impossible to create a security policy for a new network segment that is secure, and at the same time, assures business continuity.

APG is also a robust tool that enables firewall professionals to tighten security on any firewall, replace old and inefficient firewall rule bases and ACLs, 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.