tufin The Security Policy Company.

Reduce Firewall Rule Permissiveness Automatically

with Automatic Policy Generator

Tufin's Automatic Policy Generator™ (APG) helps you optimize your firewall rule bases, using traffic history to design least-privilege rule sets that block communications from systems that don't regularly require access.

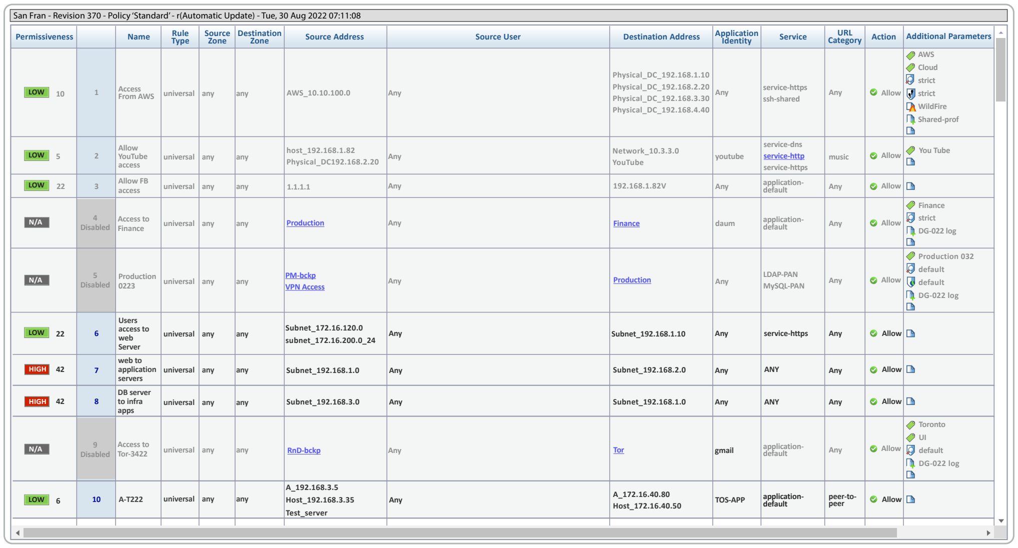
The APG can also accelerate the creation of a new rule base for new firewalls or adding an interface to a firewall.

The APG analyzes firewall logs to determine actual business practices, and replaces overly permissive rules with more granular rules, where overly permissive is defined as allowing access that is unused. Tufin customers can run an APG job on a rule which will watch actual business traffic for a specified amount of time and then suggest a recommended set of rules to reduce the permissiveness of the existing rule, or users can import logs to provide Tufin the traffic baseline data.

> **"Tufin showed us everything we were doing wrong."**
>
> — G2 Product Review, Enterprise >1,000 Employees

Optimize Existing Firewalls - Rule Audit

Restrict existing rules that are too permissive. By analyzing the rule base, the APG can identify the permissive rules on a firewall and provide alternatives that are more accurate. The APG can be run on an entire firewall rule base, a specific section, or just one rule.



San Fran - Revision 370 - Policy 'Standard' - r(Automatic Update) - Tue, 30 Aug 2022 07:11:08

Permissiveness		Name	Rule Type	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application Identity	Service	URL Category	Action	Additional Parameters
LOW 10	1	Access From AWS	universal	any	any	AWS_10.10.100.0	Any	Physical_DC_192.168.1.10 Physical_DC_192.168.2.20 Physical_DC_192.168.3.30 Physical_DC_192.168.4.40	Any	service-https ssh-shared	Any	✓ Allow	AWS Cloud strict strict WildFire Shared-prof
LOW 5	2	Allow YouTube access	universal	any	any	host_192.168.1.82 Physical_DC192.168.2.20	Any	Network_10.3.3.0 YouTube	youtube	service-dns service-http service-https	music	✓ Allow	You Tube
LOW 22	3	Allow FB access	universal	any	any	1.1.1.1	Any	192.168.1.82V	Any	application-default	Any	✓ Allow	
N/A	4 Disabled	Access to Finance	universal	any	any	Production	Any	Finance	daum	application-default	Any	✓ Allow	Finance strict DG-022 log
N/A	5 Disabled	Production 0223	universal	any	any	PM-bckp VPN Access	Any	Production	Any	LDAP-PAN MySQL-PAN	Any	✓ Allow	Production 032 default default DG-022 log
LOW 22	6	Users access to web Server	universal	any	any	Subnet_172.16.120.0 subnet_172.16.200.0_24	Any	Subnet_192.168.1.10	Any	service-https	Any	✓ Allow	
HIGH 42	7	web to application servers	universal	any	any	Subnet_192.168.1.0	Any	Subnet_192.168.2.0	Any	ANY	Any	✓ Allow	
HIGH 42	8	DB server to infra apps	universal	any	any	Subnet_192.168.3.0	Any	Subnet_192.168.1.0	Any	ANY	Any	✓ Allow	
N/A	9 Disabled	Access to Tor-3422	universal	any	any	RnD-bckp	Any	Tor	gmail	application-default	Any	✓ Allow	Toronto UI default DG-022 log
LOW 6	10	A-T222	universal	any	any	A_192.168.3.5 Host_192.168.3.35 Test_server	Any	A_172.16.40.80 Host_172.16.40.50	TOS-APP	application-default	peer-to-peer	✓ Allow	

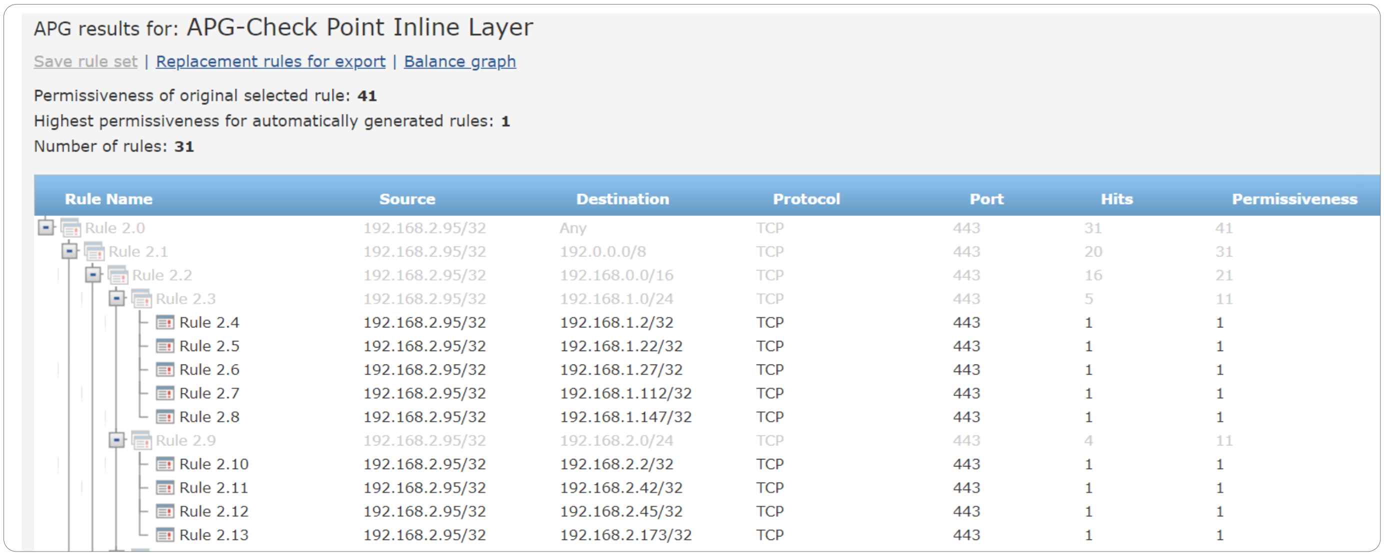
The APG identifies the permissiveness level of each 'accept' rule, on a scale from 1 to 100. Permissiveness measures how widely a rule is defined:

- A rule with one source host, one destination host and one service has the smallest value - **1**
- A rule with Source "ANY", Destination "ANY" and Protocol "ANY" has the highest value - **100**

Features

- Can analyze real time logs or users can import logs
- Run APG on an entire rule base, a section, or one rule
- At-a-glance view of critical metrics
- Rule base suggestions are defined to:
  - Approximate a least-privilege state based on traffic history
  - Optimize for high performance
  - Facilitate easy management

> **"APG allowed us to see all the rules that were too permissive and gave us a quick and easy way to resolve those with new rules that were tighter."**
>
> — G2 Product Review, Enterprise >1,000 Employees



APG results for: APG-Check Point Inline Layer

Save rule set | Replacement rules for export | Balance graph

Permissiveness of original selected rule: **41**
Highest permissiveness for automatically generated rules: **1**
Number of rules: **31**

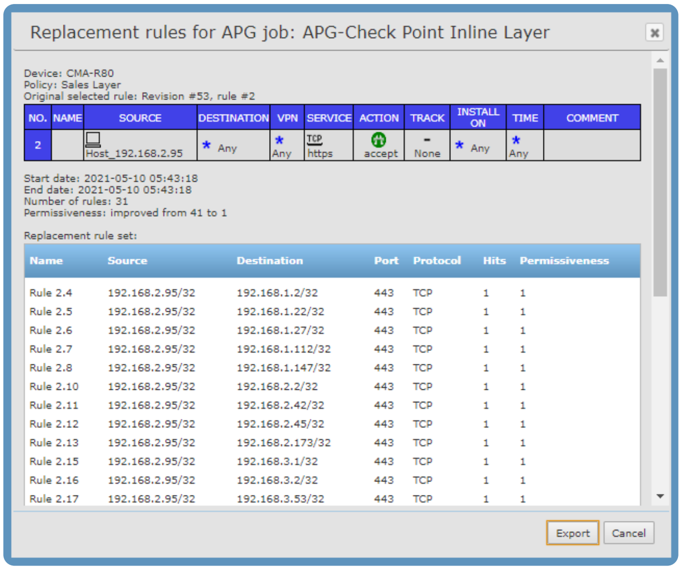
Rule Name	Source	Destination	Protocol	Port	Hits	Permissiveness
Rule 2.0	192.168.2.95/32	Any	TCP	443	31	41
Rule 2.1	192.168.2.95/32	192.0.0.0/8	TCP	443	20	31
Rule 2.2	192.168.2.95/32	192.168.0.0/16	TCP	443	16	21
Rule 2.3	192.168.2.95/32	192.168.1.0/24	TCP	443	5	11
Rule 2.4	192.168.2.95/32	192.168.1.2/32	TCP	443	1	1
Rule 2.5	192.168.2.95/32	192.168.1.22/32	TCP	443	1	1
Rule 2.6	192.168.2.95/32	192.168.1.27/32	TCP	443	1	1
Rule 2.7	192.168.2.95/32	192.168.1.112/32	TCP	443	1	1
Rule 2.8	192.168.2.95/32	192.168.1.147/32	TCP	443	1	1
Rule 2.9	192.168.2.95/32	192.168.2.0/24	TCP	443	4	11
Rule 2.10	192.168.2.95/32	192.168.2.2/32	TCP	443	1	1
Rule 2.11	192.168.2.95/32	192.168.2.42/32	TCP	443	1	1
Rule 2.12	192.168.2.95/32	192.168.2.45/32	TCP	443	1	1
Rule 2.13	192.168.2.95/32	192.168.2.173/32	TCP	443	1	1

Adding a New Firewall to Your Network

If you do not yet have a firewall policy in place, you can begin by configuring a relatively permissive policy, and leave it in place long enough to produce logs. The APG can then translate these logs into a secure, optimized rule base.

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 tradeoff between the degree of permissiveness, and the size of the rule base, the APG allows you to interactively determine how granular you want the rule base to be.



Replacement rules for APG job: APG-Check Point Inline Layer

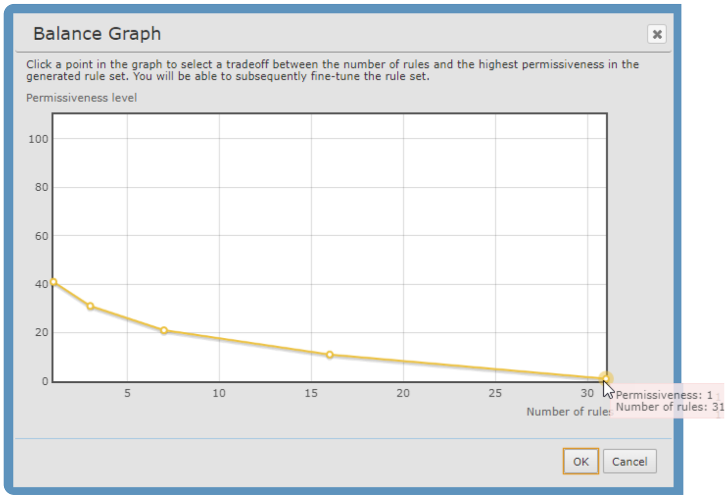
Device: CMA-R80
Policy: Sales Layer
Original selected rule: Revision #53, rule #2

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
2		Host_192.168.2.95	* Any	* Any	TCP https	accept	- None	* Any	* Any	

Start date: 2021-05-10 05:43:18
End date: 2021-05-10 05:43:18
Number of rules: 31
Permissiveness: improved from 41 to 1

Replacement rule set:

Name	Source	Destination	Port	Protocol	Hits	Permissiveness
Rule 2.4	192.168.2.95/32	192.168.1.2/32	443	TCP	1	1
Rule 2.5	192.168.2.95/32	192.168.1.22/32	443	TCP	1	1
Rule 2.6	192.168.2.95/32	192.168.1.27/32	443	TCP	1	1
Rule 2.7	192.168.2.95/32	192.168.1.112/32	443	TCP	1	1
Rule 2.8	192.168.2.95/32	192.168.1.147/32	443	TCP	1	1
Rule 2.10	192.168.2.95/32	192.168.2.2/32	443	TCP	1	1
Rule 2.11	192.168.2.95/32	192.168.2.42/32	443	TCP	1	1
Rule 2.12	192.168.2.95/32	192.168.2.45/32	443	TCP	1	1
Rule 2.13	192.168.2.95/32	192.168.2.173/32	443	TCP	1	1
Rule 2.15	192.168.2.95/32	192.168.3.1/32	443	TCP	1	1
Rule 2.16	192.168.2.95/32	192.168.3.2/32	443	TCP	1	1
Rule 2.17	192.168.2.95/32	192.168.3.53/32	443	TCP	1	1



Balance Graph

Click a point in the graph to select a tradeoff between the number of rules and the highest permissiveness in the generated rule set. You will be able to subsequently fine-tune the rule set.

www.tufin.com

The Security Policy Company.