



Approval Process Automation

Segregation of duties requires that if firewall policy change is implemented by a person or team there must be another person or team that will do the necessary judgement or evaluation on the request. This is also called approval process for firewall policy change activity. The approval is a process including corporate policy check and if the request is not in accordance with the corporate security policy the request would be rejected and sent to the requester to make change on the request.

How to be sure that approval is done correct?

Opinnate has a mechanism to make sure approval is done correct

It is possible for approver to make mistakes during approval. They may not look at policy documents each time and forget the core principles when approving. It is quite possible that firewall policy table becomes irrelevant to the security policies in quite a short time.

		Destination					
		asa	FG4	FDS	PA	XEOS	lg1
Source	asa	⊘ ⚙	i ⚙	N/A ⚙	✓ ⚙	i ⚙	N/A ⚙
	FG4	✓ ⚙	✓ ⚙	i ⚙	✓ ⚙	i ⚙	N/A ⚙
	FDS	⊘ ⚙	i ⚙	⊘ ⚙	✓ ⚙	N/A ⚙	N/A ⚙
	PA	i ⚙	✓ ⚙	⊘ ⚙	⊘ ⚙	i ⚙	N/A ⚙
	XEOS	⊘ ⚙	⊘ ⚙	✓ ⚙	⊘ ⚙	N/A ⚙	N/A ⚙
	lg1	N/A ⚙	N/A ⚙	N/A ⚙	N/A ⚙	N/A ⚙	N/A ⚙

Benefits

- Being sure policies are applied
- Hardening firewall rules
- Being more secure
- Faster approval process
- Effort gain on approval activity
- Agility in security

Corporate security policy be visualized on a matrix

Opinnate makes it possible to import corporate security policy of any organization into a corporate security policy matrix. With the aid of this policy matrix relations between each zone in the environment be defined. In every request coming to the system this policy checking is to be done to give information about the compliancy of the request to the policies. An automatic way of checking policies each time needed. This matrix can also be updated any time needed.



Automatic way of approving requests

Opinnate makes security approval for policy changes an automatic process

If the request totally compliant to the security policies, then there may not be additional approver control on the request. In that case the approval can be done automatically without any effort on approval site. This will make approver team to focus on other issues more important. This automatic process may necessitate the approver team make regular controls on the policies more often instead of longer period reviews. And this makes IT security teams to be more agile for the changes both on business site and security industry.

The image shows a user interface for adding a new role. It features a modal dialog box titled "Add New Role." with a close button (X). Inside the dialog, there are two text input fields: "Role Name" (containing the letter 'I') and "Description". Below these fields is a blue button labeled "ADD IP".

Below the dialog box, there is a table of IP addresses. The table has a "New IP" input field with an "ADD" button next to it. The table contains four rows, each with an IP address and a red "X" button for deletion.

New IP	ADD
192.168.20.0/25	X
192.168.16.0/24	X
192.168.66.0/27	X
192.168.33.0/24	X

With Opinnate increase your security policies maturity level every time you need

Updating corporate policies is a fun and easy process that can be done regularly by just the IT Security teams in accordance with the segregation of duties principle