Administrative Roles and Permissions

https://campus.barracuda.com/doc/91985189/

In order to create and manage application and rule entries on the Firewall Policy Manager, users are assigned administrative roles. A mapping functionality allows you to assign roles in the Firewall Policy Manager to corresponding groups in Active Directory. This requires a base OU from Active Directory below which is searched. The groups can be created in the web interface with any desired names and mapped to the corresponding AD groups. After successful connection, the group can be equipped with authorizations.

Administrative Roles

The administrative role a user or group belongs to defines the scope and sets the permissions for what content they have access to. The role also decides if administrators are allowed to create policies, have read or write access, and can change the status of the Policy Manager ticket during the process of creation and assignment. In general, there are five predefined roles available:

- **Application Owner / Rule Applicant** – Every user with a Firewall Policy Manager login permission has the possibility to create applications or rules and assign them to the next instance with status "Assigned to Architect".
- **Architect** – A user with the role 'Architect' can review the ticket and add comments. After the check, they can change the status to "Approved Architect" or "Rejected" and assign the ticket to the next instance.
- **Operator** – A user with the role 'Operator' reviews the application or rule, makes recommendations, and passes the ticket on with the status "Evaluated Operator".
- **CISO** – A user with the role 'CISO' makes final decisions, changes the ticket status to "Approved CISO" and assigns the ticket back to CISO. CISO employees are also responsible for the manual implementation of a rule.

Firewalls and Control Centers are only allowed configuration and write access by members of Operator. Read access is not restricted for other groups.

For a detailed explanation of interactions of administrative roles within the procedure of ticket creation and assignment, see Application and Rules Assignment.

Configuration Access

User groups have access to the Firewall Policy Manager configuration according to their configured

rule:

	Application Owner	Rule Applicant	Architect	Operator	CISO
Configuration Tab					
Applications	YES	YES	YES	YES	YES
Rules	YES	YES	YES	YES	YES
Dependencies	NO	NO	NO	YES	NO
Advanced	NO	NO	NO	NO	NO

Email Notifications

During the ticketing process, the Firewall Policy Manager sends out notifications to different administrator groups. For example, at the end of a rule implementation, a notification will be sent to everyone previously involved.

> For automatic notifications to be sent, an email server must be configured. The following information is required: server name, server port and IP address, username, and password.

Notifications about updates and status changes are sent to the users and groups defined as owners of applications or rules as follows:

	Application Owner	Rule Applicant	Architect	Operator	CISO
Applications					
Status change to Assigned Architect	NO	NO	YES	NO	NO
Status change to Approved Architect	YES	NO	NO	YES	NO
Status change to Evaluated Architect	YES	NO	NO	NO	YES
Status change to Approved CISO	YES	NO	NO	YES	NO
Status change to Rejected	YES	NO	NO	NO	NO
New comment added	YES	NO	YES	YES	YES
Rules					
Status change to Assigned Architect	NO	NO	YES	NO	NO
Status change to Approved Architect	NO	NO	NO	YES	NO
Status change to Evaluated Architect	NO	NO	NO	NO	YES
Status change to Approved CISO	NO	NO	NO	YES	NO

Status change to Implemented	NO	YES	NO	NO	NO
Status change to Verified	NO	YES	NO	NO	NO
Status change to Rejected	NO	YES	YES	YES	YES
New comment added	NO	YES	YES	YES	YES