Application and Rules Assignment

https://campus.barracuda.com/doc/91985191/

The Firewall Policy Manager web interface allows users with dedicated roles to create and process applications and rules using a built-in ticketing system. As soon as the ticket status for an application is "Closed", an application can be assigned to rules, which, in a subsequent process, can be applied to firewalls in your network. The workflow for creating and processing applications is very similar to the procedure for creating firewall rules; however, the latter includes firewall assignment.

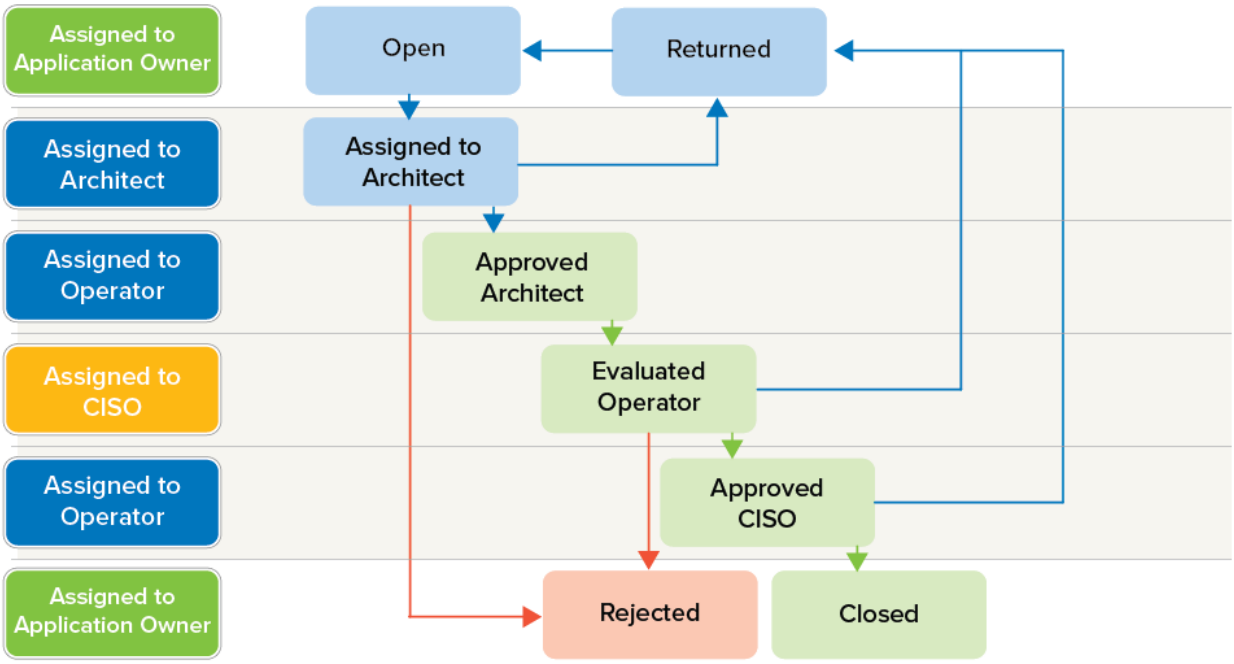
Application Assignment Process

The **Applications** tab lets administrators create and process applications. The procedure for creating and processing applications can be seen as follows:

1. The **Application Owner** creates a new application and adds information such as name, IP address, network dependency, and security evaluation. At the time of creation, the status of the entry is "Open", which represents the application. The application status can then be changed to "Assigned Architect".
2. **Architect** opens the application and adds comments to the request, after which the ticket status is changed to "Approved Architect" or "Rejected". **Architect** passes the ticket on to **Operator**.
3. **Operator** passes the ticket on to **CISO** with the status "Evaluated Operator".
4. **CISO** ultimately decides on the release of the application. The ticket then goes to the status "Approved CISO" and gets assigned back to the application owner, who changes the status to "Closed". From this point on, the application can be selected when creating a firewall rule. Otherwise, **CISO** can also reject the application and return it to the application owner with status "Rejected". In the case of rejected applications with the status "Rejected", the **Application Owner** can complete the information and carry out the operation again.

All participants have the opportunity to make comments and additions. Every change of the assignee and the status is logged and is visible.

The following illustration shows the assignment definition when a new application gets created with the status "Open" and explains the processing workflow:



For detailed information on rules creation and assignment, see How to Create Applications.

Rules Assignment Process

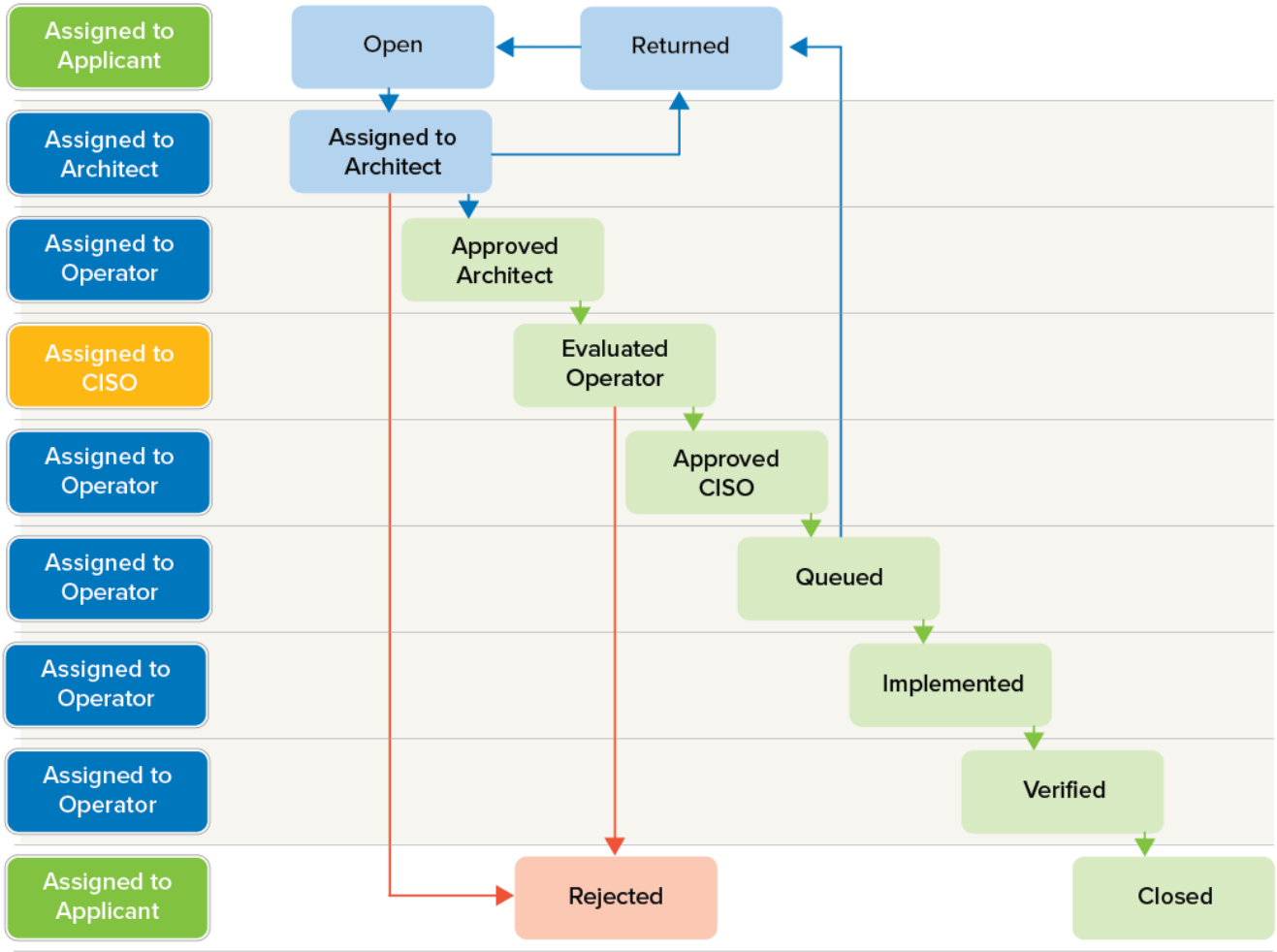
The **Rules** tab lets users create and process firewall rules. The administrator who starts the rule request process, selects application and asset and fills in the required information such as name and description. After this process, the request is sent to Architect. Architect checks the rule information, commits a security assessment, and forwards the rule request to Operator. If the rule gets approved, it can be submitted to the Firewall Control Center. The procedure of creating and processing rules can be seen as follows:

1. The **Rule Applicant** creates a new firewall rule and adds information such as application, asset, source, and destination. The rule status can then be changed to "Assigned Architect".
2. **Architect** opens the rule and can assign it to themself. It is possible to comment on the request, after which the status is changed to "Approved Architect" or "Rejected". **Architect** passes the ticket on to **Operator**.
3. **Operator** passes the ticket on to **CISO** with the status "Evaluated Operator". In this step, the Firewall Policy Manager creates an automatic safety assessment, which is sent to **CISO** as a recommendation.
4. **CISO** ultimately decides on the release of the rule, the rule goes into the status "Approved CISO" and gets assigned back to **Operator**. **CISO** employees are responsible for the manual implementation of the rule. As soon as the rule has been assigned to a Control Center, it gets the status "Queued". **CISO** employees remain responsible. When the rule has been successfully

submitted to the Control Center and can be accessed on CC-managed firewall units, the ticket status changes to "Implemented". A notification will be sent to everyone previously involved. Otherwise, for example, if rule transfer to a Control Center fails, **CISO** can also reject the ticket and assign it back to the owner with the status "Rejected". In the case of rejected ticket with the status "Rejected", the owner can complete the information and carry out the operation again.

All participants have the opportunity to make comments and additions. Every change of the assignee and the status is logged and is visible.

The following figure shows the assignment definition when a new rule gets created with the status "Open" and explains the processing workflow:



For detailed information on rules creation and assignment, see How to Create Rules.

Figures