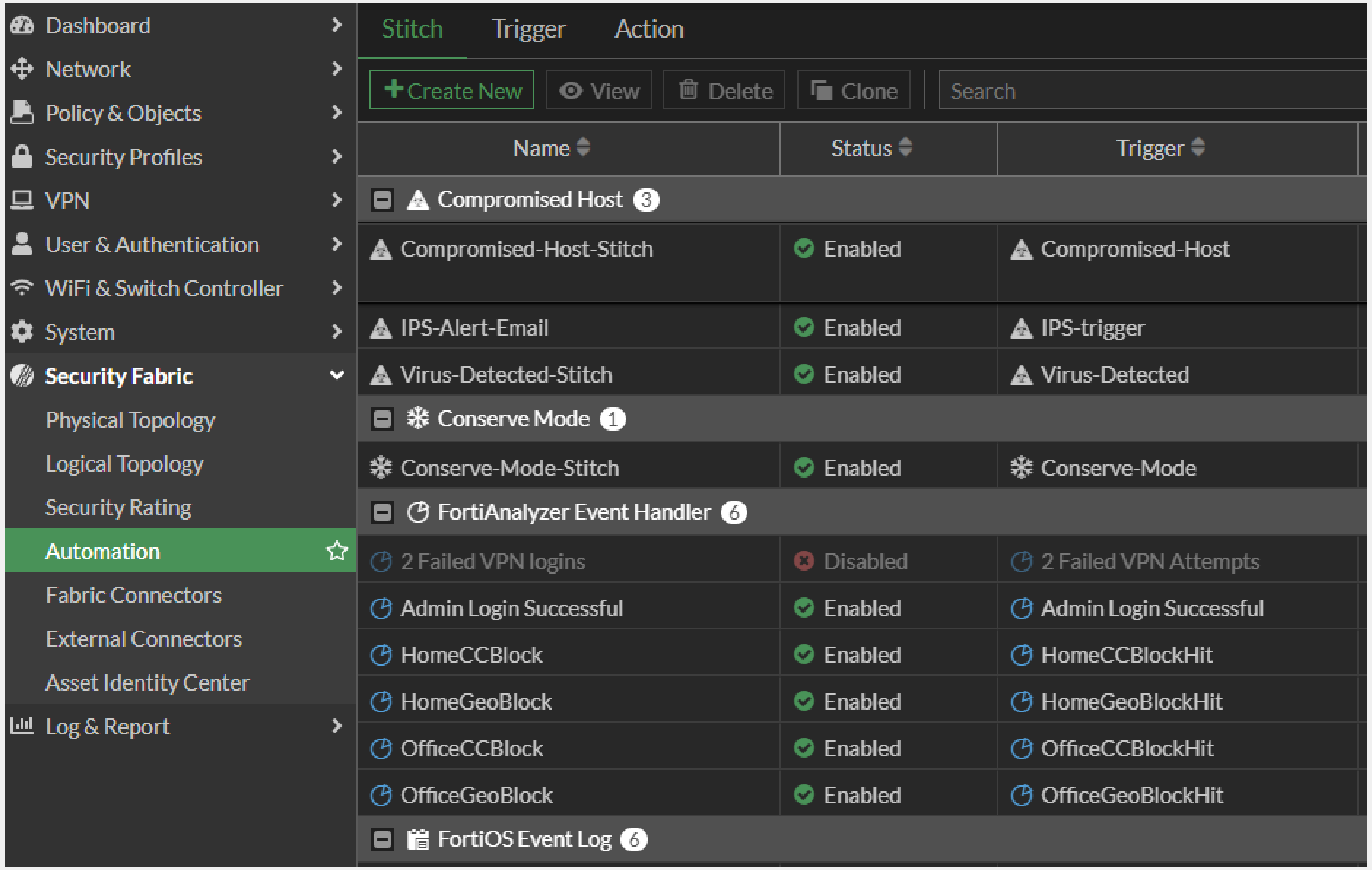
FORTINET

April SUNY Office Hours

FortiGate Automation

Automation Overview

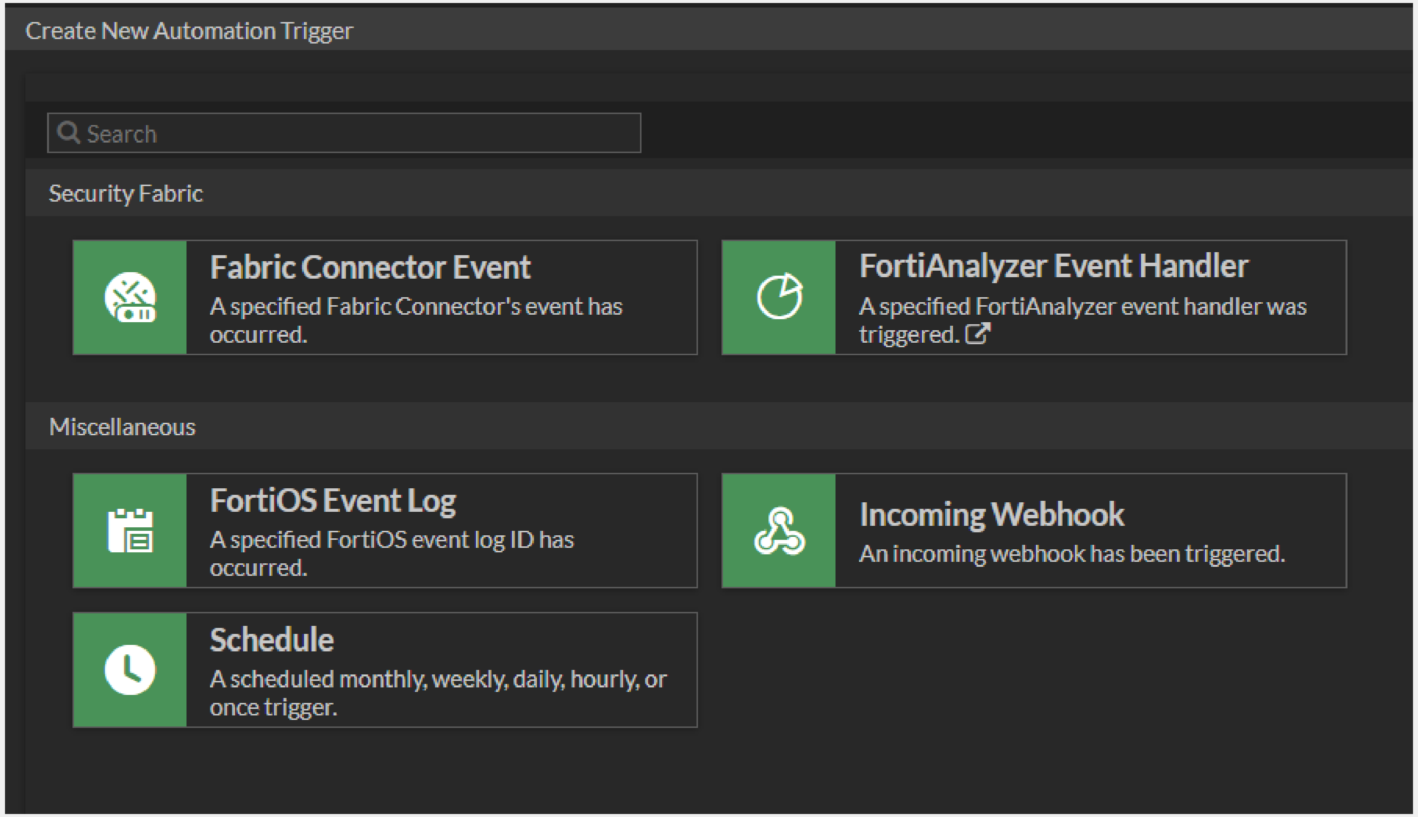
- Free option to create automated actions to respond to network and system events
- Schedule after hours changes
- Multiple different notification options – email, Teams, etc
- Pairs a Trigger with an Action
- FortiAnalyzer adds additional event filtering capabilities



Name	Status	Trigger
⊟ Compromised Host 3		
Compromised-Host-Stitch	✓ Enabled	Compromised-Host
IPS-Alert-Email	✓ Enabled	IPS-trigger
Virus-Detected-Stitch	✓ Enabled	Virus-Detected
⊟ Conserve Mode 1		
Conserve-Mode-Stitch	✓ Enabled	Conserve-Mode
⊟ FortiAnalyzer Event Handler 6		
2 Failed VPN logins	✗ Disabled	2 Failed VPN Attempts
Admin Login Successful	✓ Enabled	Admin Login Successful
HomeCCBlock	✓ Enabled	HomeCCBlockHit
HomeGeoBlock	✓ Enabled	HomeGeoBlockHit
OfficeCCBlock	✓ Enabled	OfficeCCBlockHit
OfficeGeoBlock	✓ Enabled	OfficeGeoBlockHit
⊟ FortiOS Event Log 6		

Automation - Triggers

- Schedule task to run, look for an event log entry, FortiAnalyzer can trigger on traffic events
- Multiple different notification options – email, Teams, etc
- Fabric connectors like FortiClient EMS can send triggers



Create New Automation Trigger

Security Fabric

Fabric Connector Event
A specified Fabric Connector's event has occurred.

FortiAnalyzer Event Handler
A specified FortiAnalyzer event handler was triggered.

Miscellaneous

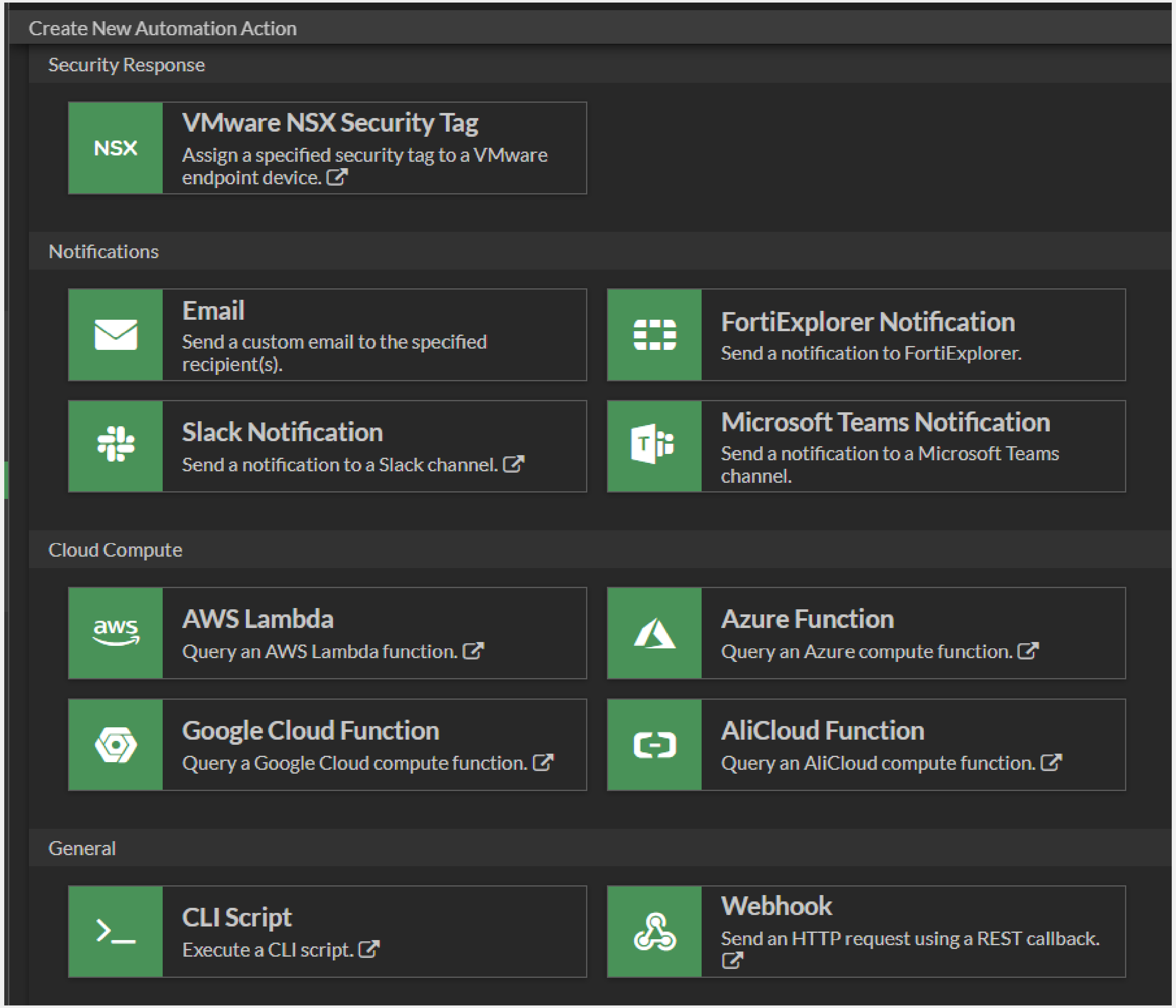
FortiOS Event Log
A specified FortiOS event log ID has occurred.

Incoming Webhook
An incoming webhook has been triggered.

Schedule
A scheduled monthly, weekly, daily, hourly, or once trigger.

Automation - Actions

- Create multiple actions to take based on trigger
- Can open ticket in ITSMs like ServiceNow
- CLI scripts can run configuration changes or state gathering like routing tables



Create New Automation Action

Security Response

VMware NSX Security Tag
Assign a specified security tag to a VMware endpoint device.

Notifications

Email
Send a custom email to the specified recipient(s).

FortiExplorer Notification
Send a notification to FortiExplorer.

Slack Notification
Send a notification to a Slack channel.

Microsoft Teams Notification
Send a notification to a Microsoft Teams channel.

Cloud Compute

AWS Lambda
Query an AWS Lambda function.

Azure Function
Query an Azure compute function.

Google Cloud Function
Query a Google Cloud compute function.

AliCloud Function
Query an AliCloud compute function.

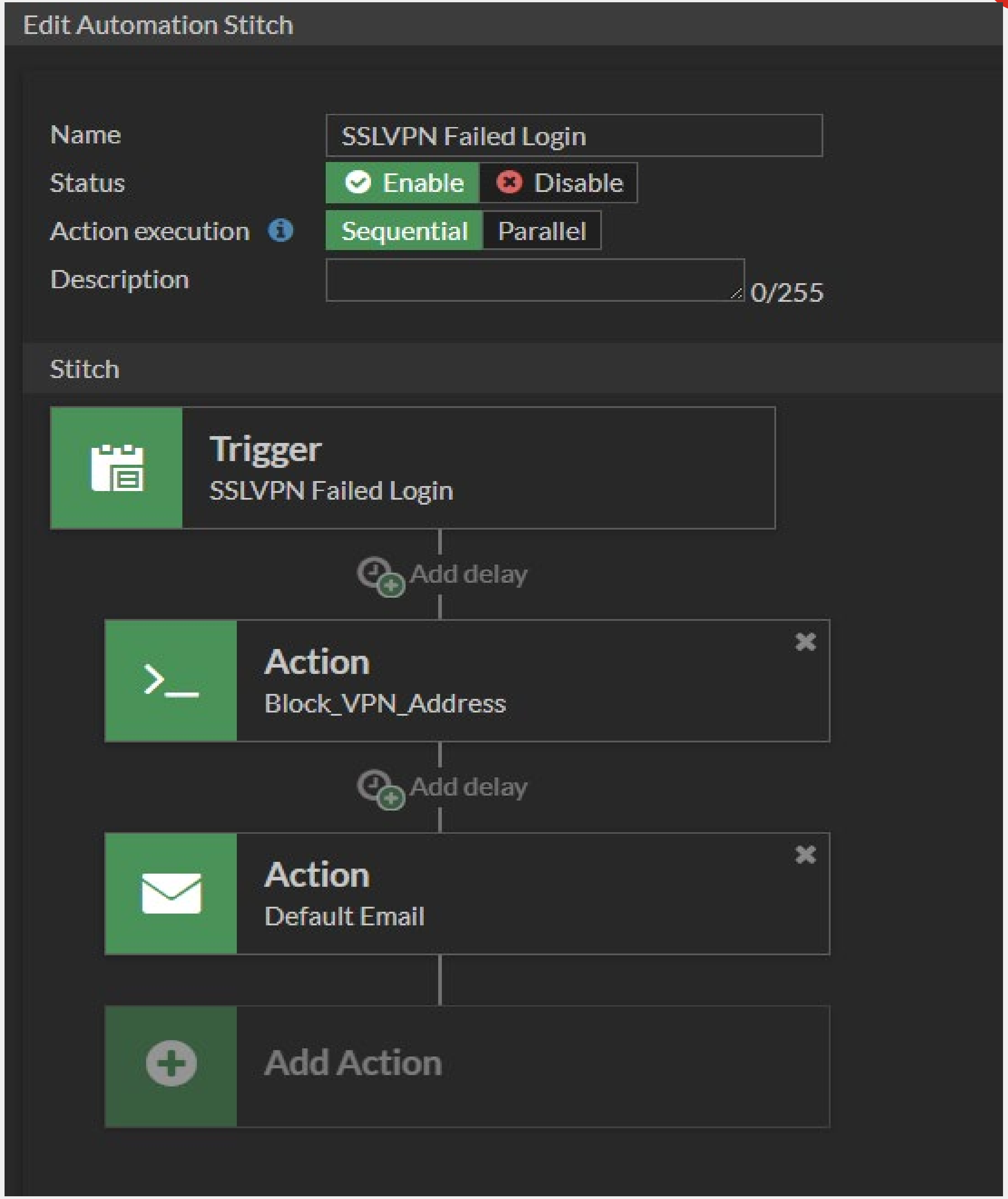
General

CLI Script
Execute a CLI script.

Webhook
Send an HTTP request using a REST callback.

Automation - Stitches

- Single trigger can have multiple actions
- Can take information from log entry and use in CLI script action
- Adding delays can be helpful for running CLI show commands and then emailing the results



Edit Automation Stitch

Name: SSLVPN Failed Login

Status: [✓ Enable] Disable

Action execution: [✓ Sequential] Parallel

Description: 0/255

Stitch

Trigger
SSLVPN Failed Login

Action
Block_VPN_Address

Action
Default Email

Resources

https://docs.fortinet.com/document/fortigate/7.6.2/administration-guide/139441/automation-stitches

https://blog.rdorman.net/triggering-homekit-automations-with-a-fortigate/

https://github.com/weis-victor/fgt-automation-stitches

https://github.com/yuriskinfo/Fortinet-tools/tree/main/Fortigate-automation-stitches

FORTINET®