Lab 4: Automation Capabilities

Exercise 3: Configuring an Event Handler With an Automation Stitch

In this exercise, you will configure an event handler on FortiAnalyzer that has the automation stitch feature enabled. You will configure a corresponding automation stitch on FortiGate that uses the event handler as an automation trigger.

When a user tries to access a blocked website, www.dropbox.com, it will trigger the automation stitch and the following will happen:

- The source IP address in the 10.200.3.0/24 network, with the exception of 10.200.3.1, is banned on the Security Fabric from accessing anything outside of its own network.
- The log entry for the relevant traffic flow is generated and emailed to an administrator.
- Diagnostics of the IP ban is generated and emailed to an administrator.

Confirm the Web Filter is Operational

Before you configure FortiAnalyzer and FortiGate, you will confirm that the web filter is blocking 10.200.3.1 and 10.200.3.219 from accessing www.dropbox.com.

To confirm the web filter is operational

1. On your bastion host, on the desktop, double-click the **Windows Server** RDP shortcut.
2. Log in with the following credentials:

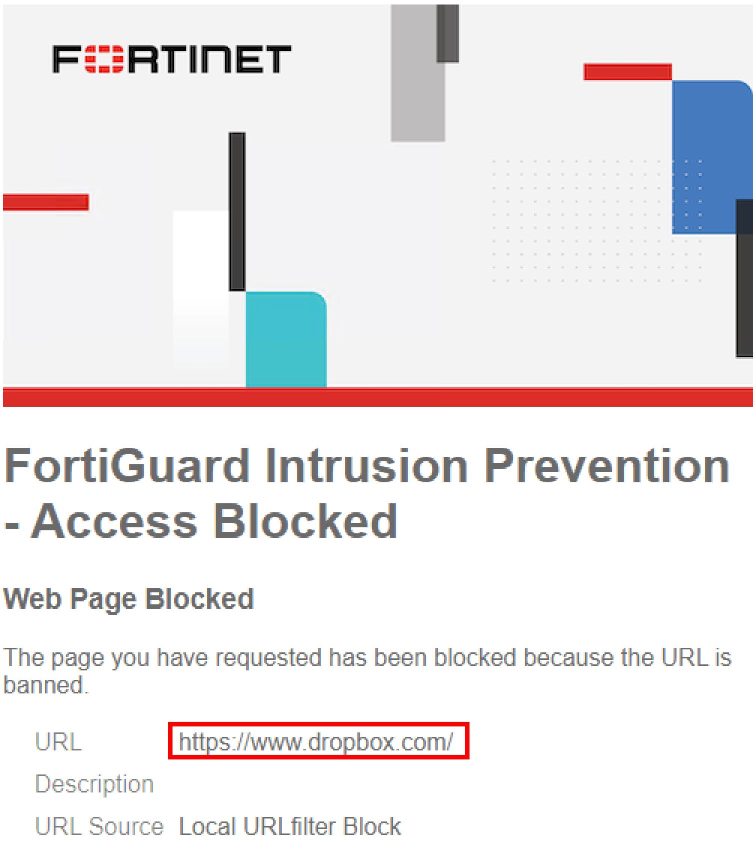
- Username: CSLAB\Administrator
- Password: Passw0rd

You may need to click **More choices** at the RDP prompt to specify the login account.

3. Open Chrome, and then go to the following URL:

www.dropbox.com

A web filter block page should appear.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

The page you have requested has been blocked because the URL is banned.

URL https://www.dropbox.com/

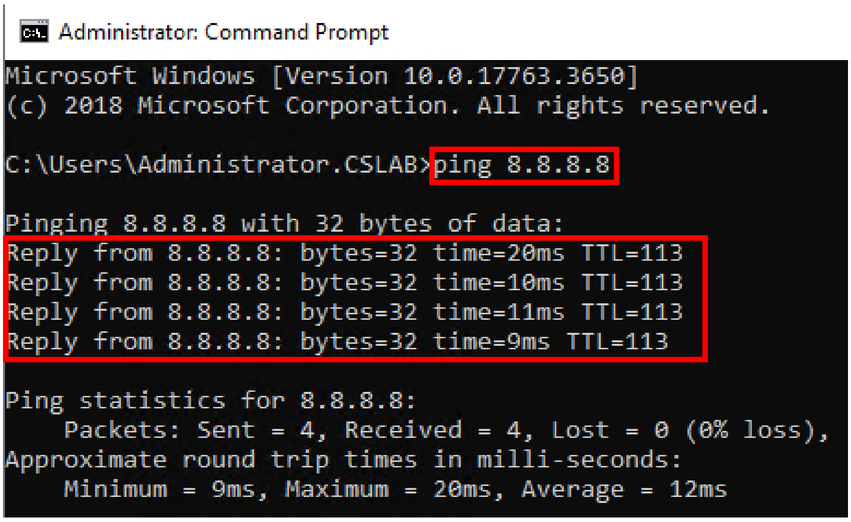
Description

URL Source Local URLfilter Block

4. Open a command prompt, and then enter the following command:

ping 8.8.8.8

The command should succeed.



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.CSLAB>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=20ms TTL=113
Reply from 8.8.8.8: bytes=32 time=10ms TTL=113
Reply from 8.8.8.8: bytes=32 time=11ms TTL=113
Reply from 8.8.8.8: bytes=32 time=9ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 20ms, Average = 12ms
```

The LAN network that these two VMs belong to blocks HTTPS traffic to the internet, with the exception of www.dropbox.com. The traffic to www.dropbox.com is blocked by the web filter profile that is configured on FortiGate-SiteB-Edge.

However, both hosts should be able to ping destinations on the internet, such as 8.8.8.8.

5. On your bastion host, on the desktop, double-click the **Windows-Client** RDP shortcut.
6. Log in with the following credentials:

- Username: CSLAB\Administrator
- Password: Passw0rd

You may need to click **More choices** at the RDP prompt to specify the login account.

7. Repeat steps 3–4 for the **Windows-Client** RDP session.
8. Keep both RDP sessions open.

Configure an Event Handler With an Automation Stitch

You will configure an event handler with the automation stitch feature enabled. You will also configure a rule that uses some regular expressions and an IP address match.

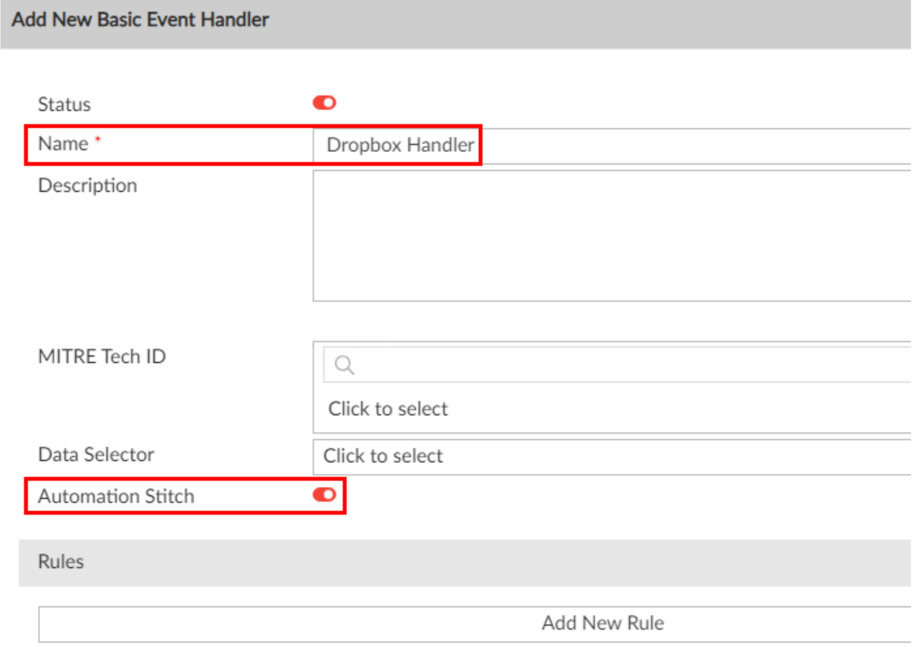
To configure an event handler with an automation stitch

1. On the bastion host, in Chrome, log in to the FAZ-SiteB GUI (10.200.4.238) with the following credentials:

- Username: admin
- Password: Fortinet1!

2. Click **Incidents & Events** > **Handlers**.
3. On the **Basic Handlers** tab, click **Create New**.
4. Configure the following settings:

Field	Value
Name	Dropbox Handler
Automation Stitch	Enabled



Add New Basic Event Handler

Status	●
Name *	Dropbox Handler
Description	
MITRE Tech ID	Click to select
Data Selector	Click to select
Automation Stitch	●

Rules

5. Click **Add New Rule**.
6. Configure the following settings:

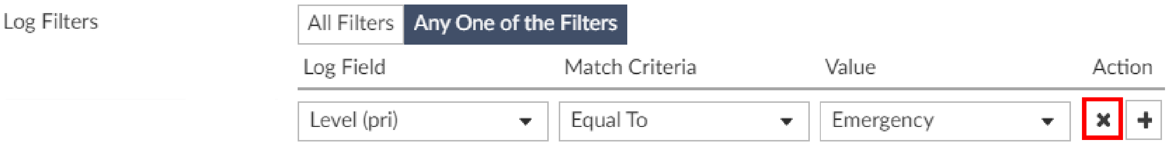
Field	Value
Name	Dropbox Rule
Log Device Type	FortiGate
Log Type	Web Filter (webfilter)
Log Field	Hostname URL (hostname) Source IP (srcip) Not in use
Log Filter by Text	url~"dropbox.com" AND srcip~"10\.200\.3\." AND srcip!=10.200.3.1
All logs were generated within < > minutes	1

The generic text filter has three conditions, and all of them must match for this rule to generate an event:

1. The URL must contain the string dropbox.com.
2. The source IP address must contain 10.200.3.
3. The source IP address must not equal 10.200.3.1.

The ~ symbol means that the characters after it are regular expressions.

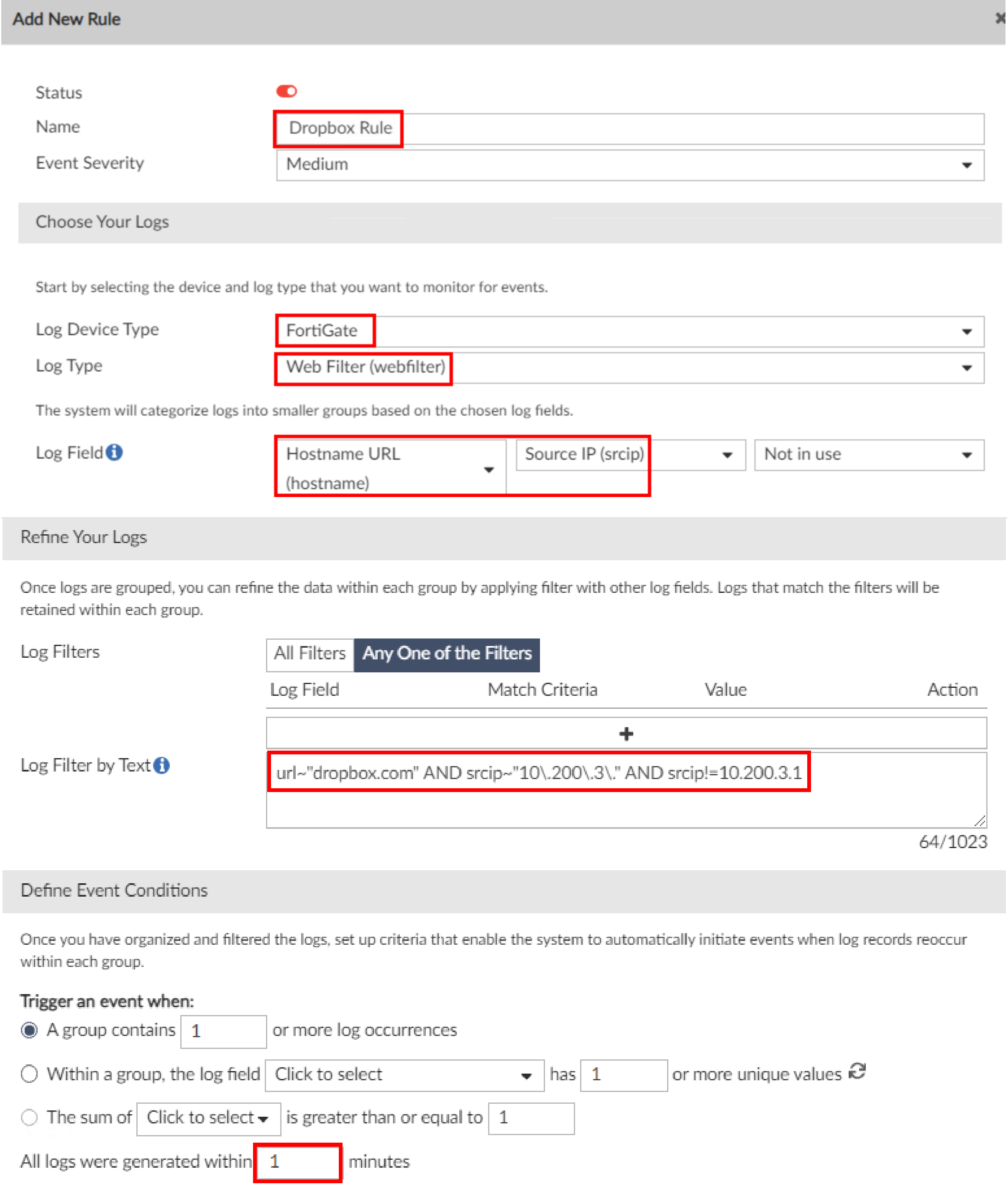
7. In the **Log Filters** field, click **x** to ensure that the default **Level (pri)** filter is removed.



Log Filters

Log Field	Match Criteria	Value	Action
Level (pri)	Equal To	Emergency	✕ +

The configuration should look like the following images:



Add New Rule

Status ●

Name: Dropbox Rule

Event Severity: Medium

Choose Your Logs

Start by selecting the device and log type that you want to monitor for events.

Log Device Type: FortiGate

Log Type: Web Filter (webfilter)

The system will categorize logs into smaller groups based on the chosen log fields.

Log Field: Hostname URL (hostname) | Source IP (srcip) | Not in use

Refine Your Logs

Once logs are grouped, you can refine the data within each group by applying filter with other log fields. Logs that match the filters will be retained within each group.

Log Filters: All Filters | Any One of the Filters

Log Field	Match Criteria	Value	Action
+			

Log Filter by Text:

```
url~"dropbox.com" AND srcip~"10\.200\.3\." AND srcip!=10.200.3.1
```

64/1023

Define Event Conditions

Once you have organized and filtered the logs, set up criteria that enable the system to automatically initiate events when log records reoccur within each group.

Trigger an event when:

● A group contains 1 or more log occurrences

○ Within a group, the log field Click to select has 1 or more unique values

○ The sum of Click to select is greater than or equal to 1

All logs were generated within 1 minutes

8. Click **OK** to save the rule.
9. Click **OK** to save the event handler.

Configuring an Automation Stitch on FortiGate

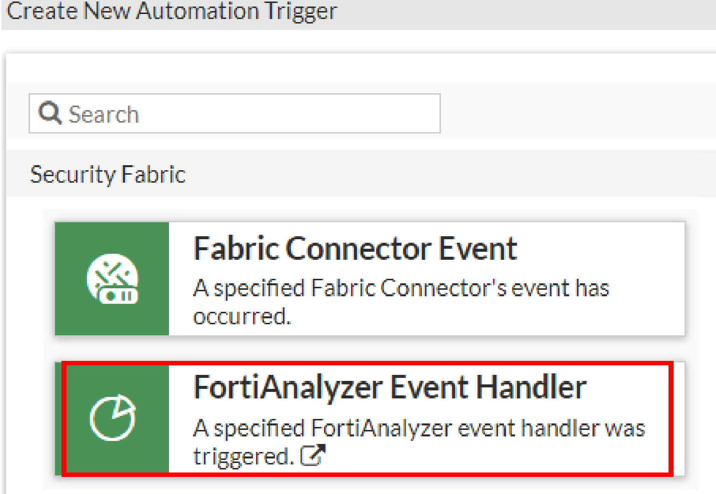
You will configure an automation stitch on FortiGate that uses **Dropbox Handler** as the trigger. You will also configure sequential actions to perform an IP ban on the offending source IP address, collect logs and diagnostics, and send them to the administrator inbox.

To configure an automation stitch trigger on FortiGate

1. On the bastion host, in Chrome, log in to the FortiGate-SiteB-Edge GUI (10.200.4.249) with the following credentials:

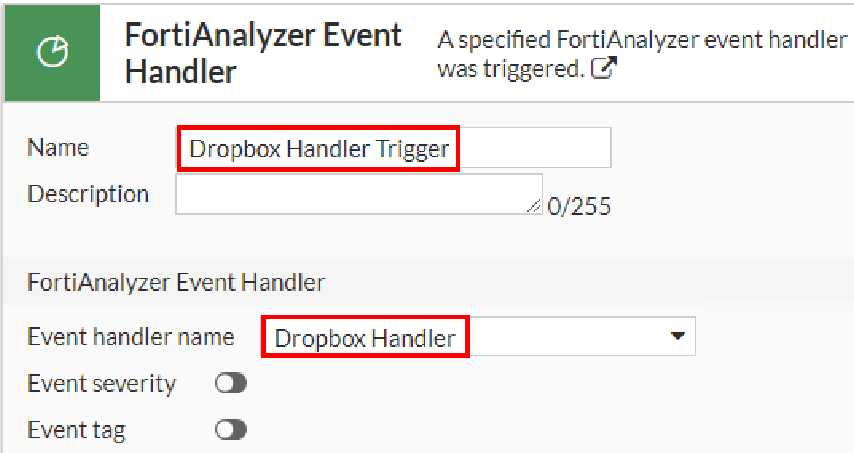
- Username: admin
- Password: Fortinet1!

2. Click **Security Fabric** > **Automation** > **Trigger**.
3. Click **Create New**.
4. Click **FortiAnalyzer Event Handler**.


Create New Automation Trigger
Search
Security Fabric
Fabric Connector Event
A specified Fabric Connector's event has occurred.
FortiAnalyzer Event Handler
A specified FortiAnalyzer event handler was triggered.

5. Configure the following settings:

Field	Value
Name	Dropbox Handler Trigger
Event handler name	Dropbox Handler


FortiAnalyzer Event Handler
A specified FortiAnalyzer event handler was triggered.
FortiAnalyzer Event Handler

Name: Dropbox Handler Trigger

Description: 0/255

Event handler name: Dropbox Handler

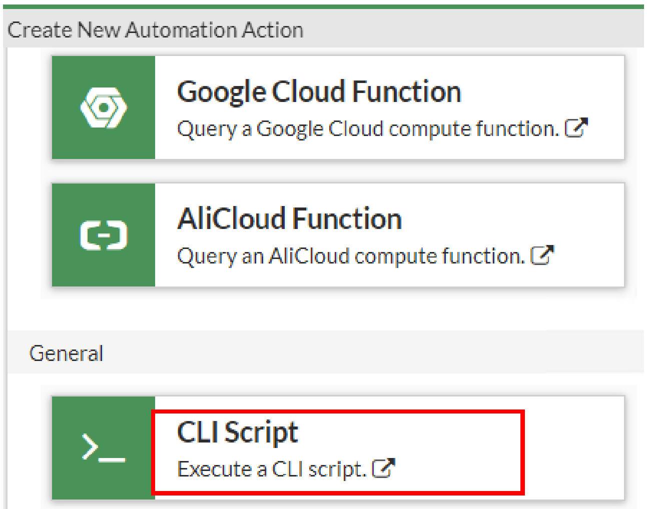
Event severity ○

Event tag ○

6. Click **OK**.

To configure automation stitch actions on FortiGate

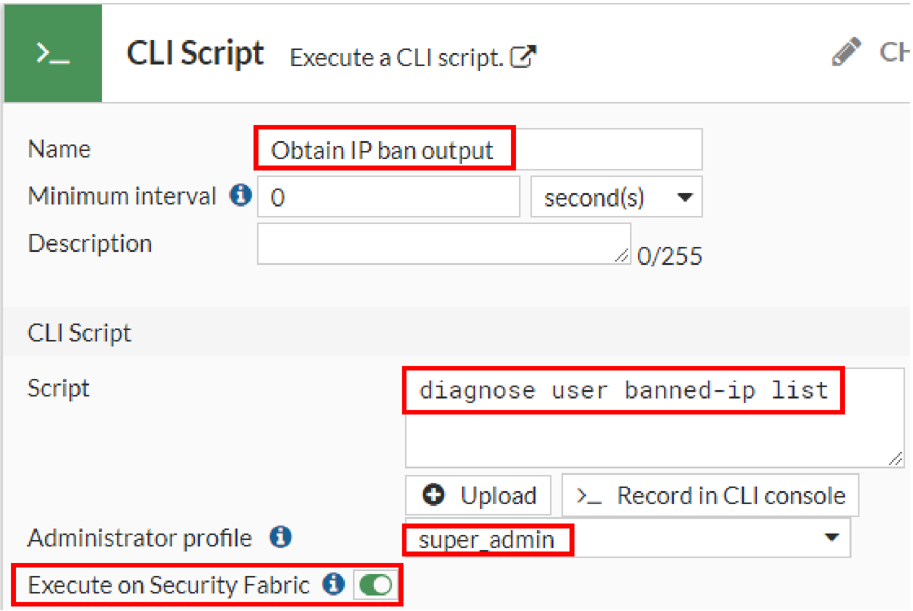
1. Click **Security Fabric** > **Automation** > **Action**.
2. Click **Create New**.
3. Click **CLI Script**.


Create New Automation Action
Google Cloud Function
Query a Google Cloud compute function.
AliCloud Function
Query an AliCloud compute function.
General
CLI Script
Execute a CLI script.

4. Configure the following settings:

Field	Value
Name	Obtain IP ban output

Field	Value
Script	diagnose user banned-ip list
Administrator profile	super_admin
Execute on Security Fabric	Enabled



Name: Obtain IP ban output

Minimum interval: 0 second(s)

Description: 0/255

CLI Script

Script:

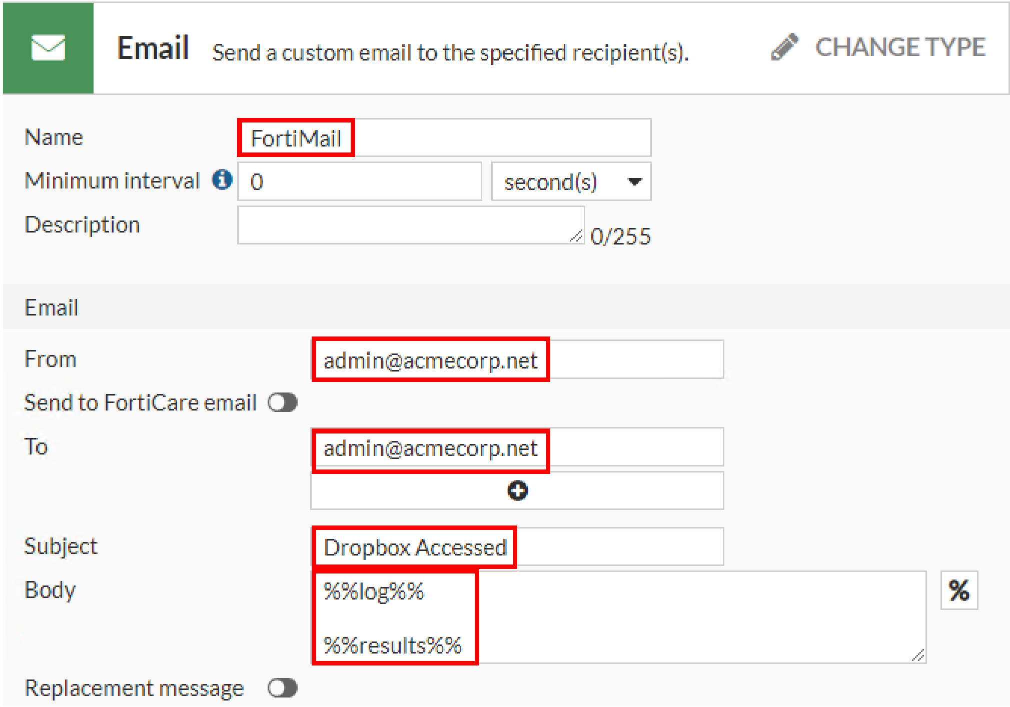
```
diagnose user banned-ip list
```

Administrator profile: super_admin

Execute on Security Fabric: ●

5. Click **OK**.
6. Click **Create New**.
7. Click **Email**.
8. Configure the following settings:

Field	Value
Name	FortiMail
From	admin@acmecorp.net
To	admin@acmecorp.net
Subject	Dropbox Accessed
Body	%%log%% %%results%%



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

Name	FortiMail
Minimum interval	0 second(s)
Description	0/255

Email

From	admin@acmecorp.net
Send to FortiCare email	
To	admin@acmecorp.net
Subject	Dropbox Accessed
Body	%%log%% %%results%%
Replacement message	

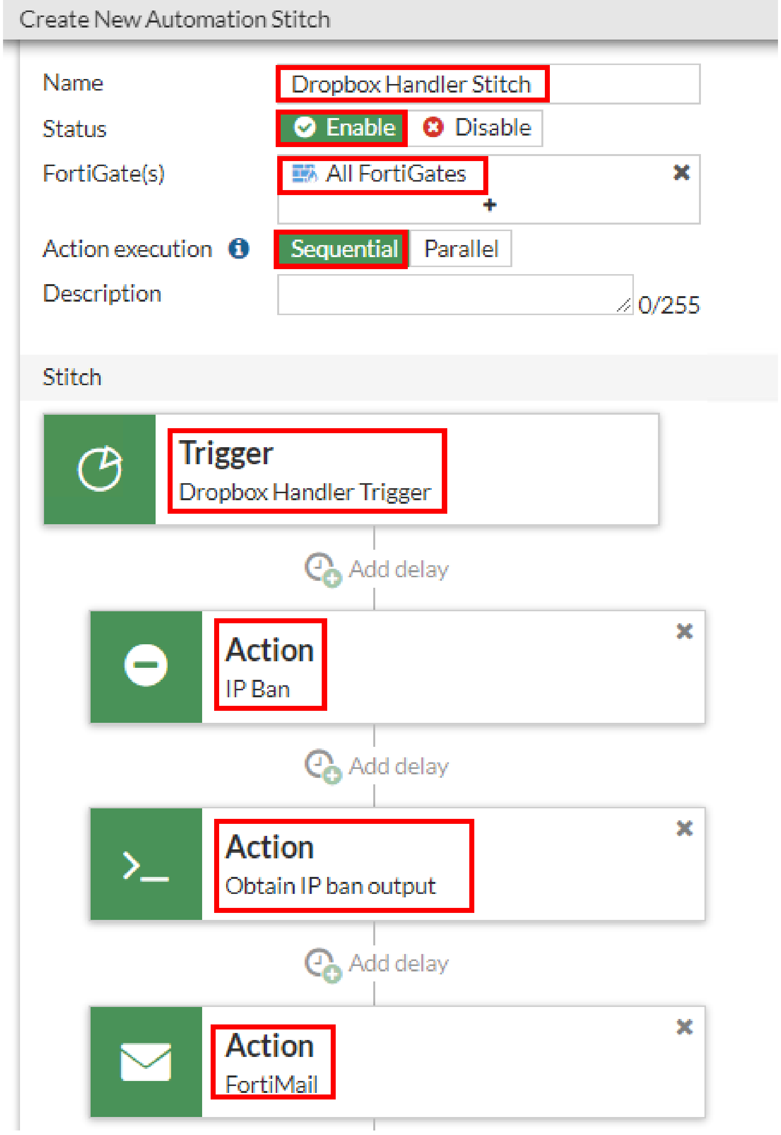
9. Click **OK**.

To configure an automation stitch on FortiGate

1. Click **Security Fabric** > **Automation** > **Stitch**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Dropbox Handler Stitch
FortiGate(s)	All FortiGates
Action execution	Sequential

4. Click **Add Trigger**, click **Dropbox Handler Trigger**, and then click **Apply**.
5. Click **Add Action**, click **IP Ban**, and then click **Apply**.
6. Click **Add Action**, click **Obtain IP ban output**, and then click **Apply**.
7. Click **Add Action**, click **FortiMail**, and then click **Apply**.



Create New Automation Stitch

Name	Dropbox Handler Stitch
Status	● Enable ○ Disable
FortiGate(s)	All FortiGates
Action execution	● Sequential ○ Parallel
Description	0/255

Stitch

Trigger
Dropbox Handler Trigger

Action
IP Ban

Action
Obtain IP ban output

Action
FortiMail

8. Click **OK**.

To test the automation stitch

1. Return to the **Windows Server** RDP session, open Chrome, and then go to the following URL:

www.dropbox.com

The web filter block page should still appear.

2. Open a command prompt.
3. Wait 1 minute, and then enter the following command:

```
ping 8.8.8.8
```

The pings should still succeed.

4. Return to the **Windows-Client** RDP session, open Chrome, and then go to the following URL:

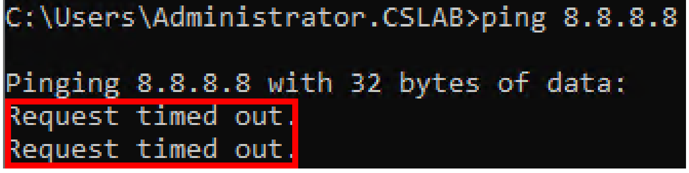
www.dropbox.com

The web filter block page should still appear.

5. Open a command prompt.
6. Wait 1 minute, and then enter the following command:

```
ping 8.8.8.8
```

The pings should now fail because the client has been banned.



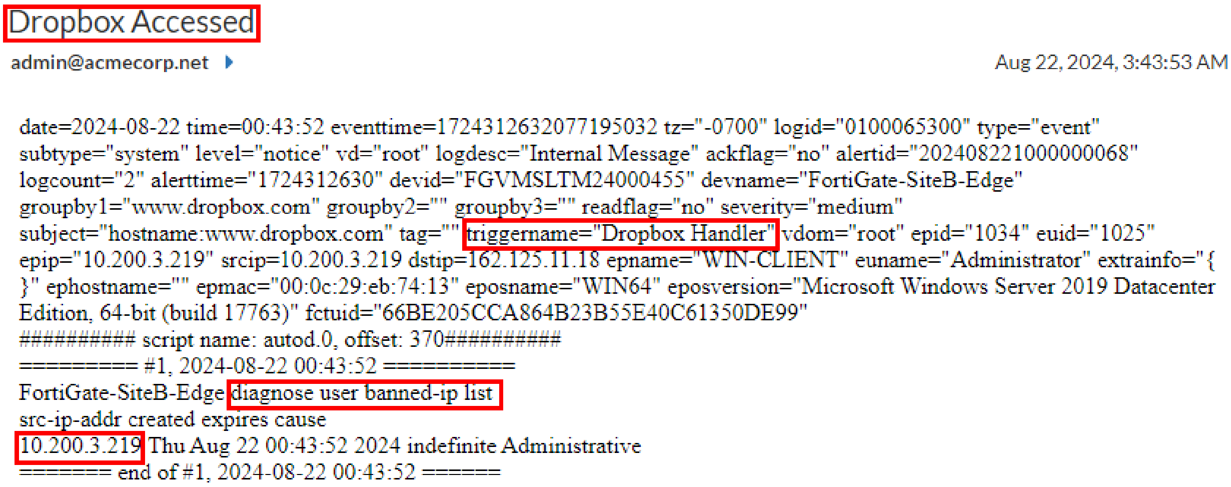
```
C:\Users\Administrator.CSLAB>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
```

7. On the bastion host, in Chrome, log in to the FortiMail (webmail) GUI (10.200.4.243) with the following credentials:

- Username: admin
- Password: Fortinet1!

8. Open the email with the subject **Dropbox Accessed**.



Dropbox Accessed

admin@acmecorp.net Aug 22, 2024, 3:43:53 AM

```
date=2024-08-22 time=00:43:52 eventtime=1724312632077195032 tz="-0700" logid="0100065300" type="event"
subtype="system" level="notice" vd="root" logdesc="Internal Message" ackflag="no" alertid="20240822100000068"
logcount="2" alerttime="1724312630" devid="FGVMSLTM24000455" devname="FortiGate-SiteB-Edge"
groupby1="www.dropbox.com" groupby2="" groupby3="" readflag="no" severity="medium"
subject="hostname:www.dropbox.com" tag="" triggername="Dropbox Handler" vdom="root" epid="1034" euid="1025"
epip="10.200.3.219" srcip=10.200.3.219 dstip=162.125.11.18 epname="WIN-CLIENT" euname="Administrator" extrainfo="{
}" ephostname="" epmac="00:0c:29:eb:74:13" eposname="WIN64" eposversion="Microsoft Windows Server 2019 Datacenter
Edition, 64-bit (build 17763)" fctuid="66BE205CCA864B23B55E40C61350DE99"
########## script name: autod.0, offset: 370##########
========= #1, 2024-08-22 00:43:52 ==========
FortiGate-SiteB-Edge diagnose user banned-ip list
src-ip-addr created expires cause
10.200.3.219 Thu Aug 22 00:43:52 2024 indefinite Administrative
======= end of #1, 2024-08-22 00:43:52 ======
```

To unban the client

1. On the bastion host, in Chrome, log in to the FortiGate-SiteB-Edge GUI (10.200.4.249) with the following credentials:

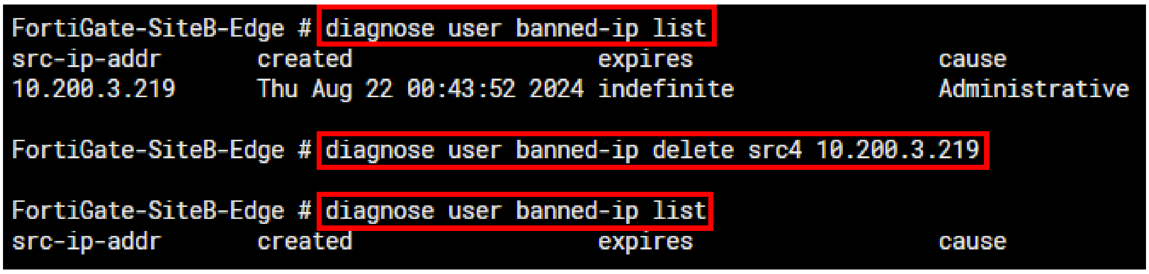
- Username: admin
- Password: Fortinet1!

2. In the upper-right corner, click the □ icon to open the CLI.
3. Enter the following commands:

```
diagnose user banned-ip list

diagnose user banned-ip delete src4 10.200.3.219

diagnose user banned-ip list
```



```
FortiGate-SiteB-Edge # diagnose user banned-ip list
src-ip-addr       created                  expires                  cause
10.200.3.219      Thu Aug 22 00:43:52 2024 indefinite               Administrative

FortiGate-SiteB-Edge # diagnose user banned-ip delete src4 10.200.3.219

FortiGate-SiteB-Edge # diagnose user banned-ip list
src-ip-addr       created                  expires                  cause
```

You are entering the first command to view the banned list, which still has the client on it. The second command is used to delete the client IP address from the banned list. The third command is to confirm the list is empty.

You can also configure an automation stitch that has a scheduled trigger to run these three commands only once on all FortiGate devices in the Security Fabric. However, for a Security Fabric with only two devices like this lab exercise, unbanning the client manually is a quick process.

4. On the bastion host, in Chrome, log in to the FortiGate-SiteB-ISFW GUI (10.200.4.234) with the following credentials:

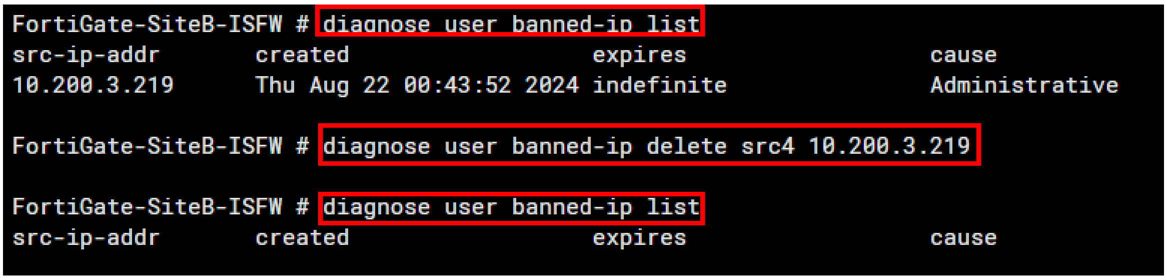
- Username: admin
- Password: Fortinet1!

5. In the upper-right corner, click the □ icon to open the CLI.
6. Enter the following commands:

diagnose user banned-ip list

diagnose user banned-ip delete src4 10.200.3.219

diagnose user banned-ip list



```
FortiGate-SiteB-ISFW # diagnose user banned-ip list
src-ip-addr       created                  expires                  cause
10.200.3.219      Thu Aug 22 00:43:52 2024 indefinite               Administrative

FortiGate-SiteB-ISFW # diagnose user banned-ip delete src4 10.200.3.219

FortiGate-SiteB-ISFW # diagnose user banned-ip list
src-ip-addr       created                  expires                  cause
```

7. Return to the **Windows-Client** RDP session, open a command prompt, and then enter the following command:

ping 8.8.8.8

The pings should succeed again.

Ensure the client is unbanned from both FortiGate devices before you finish this exercise.

LAB-4 > Configuring an Event Handler With an Automation Stitch

Outline

preview

-