FORTINET AND IBM RESILIENT

Overview ................................................................. 3
Deployment Prerequisites ........................................... 3
Architecture Overview ................................................ 3
FortiAnalyzer Configuration ........................................ 4
IBM Resilient Configuration ......................................... 7
Summary ................................................................. 10
OVERVIEW

Fortinet (NASDAQ: FTNT) is a global provider of high-performance network security and specialized security solutions that provide our customers with the power to protect and control their IT infrastructure. Our purpose-built, integrated security technologies, combined with our FortiGuard security intelligence services, provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape.

The Fortinet Security Fabric brings together all components in your network. It is Broad, Powerful and Automated. In addition to Fortinet products, the Security Fabric also integrates with 3rd Party partners to extend the power of the Security Fabric to other parts of an organization. For more information regarding our Security Fabric Partners, please refer to our Technology Alliances here: [https://www.fortinet.com/partners/partnerships/alliance-partners.html](https://www.fortinet.com/partners/partnerships/alliance-partners.html)

IBM Resilient Incident Response Platform (IRP) is the leading platform for orchestrating and automating incident response processes. IBM Resilient IRP quickly and easily integrates with your organization’s existing security and IT investments. It makes security alerts instantly actionable, provides valuable intelligence and incident context, and enables adaptive response to complex cyber threats.

DEPLOYMENT PREREQUISITES

1. Fortinet FortiAnalyzer version 6.x (tested with version 6.0.0)
2. IBM Resilient version 30.x (tested with version 30.0.3476)
   a. With Email Connector version 2.2 installed

ARCHITECTURE OVERVIEW
FORTIANALYZER CONFIGURATION

Create and configure an Email Server.

From System Settings go to Mail Server > Create New.

Enter a name to identify the mail server, the hostname or IP address of your mail server and the SMTP port (typically 25).

Be sure to enable Authentication if your mail server requires it. Then, enter a valid Email address and password for the Account.

Click OK when done.
Configure FortiAnalyzer to send Email Alerts when certain Events occur.

Click System Settings from the top left then choose Event Manager
From this view you can see there was an HTTP Event specifically about Application Control. On the right, the Handler is where Email Alerting is configured.

![Event Manager](image)

In this example we will configure an Email Alert to be sent when there is an Admin logon failure via SSH.

Click Collapse All.

![Event Manager](image)

Then locate the Event User login from SSH. Click Local Device Event under the Handler.

![Event Manager](image)

Enable Send Email Alert under Notifications. Enter the Email address you want to send Alerts to. Enter the Email address you want to use as the sender address. Enter a Subject for the Email. Lastly, under Email Server, choose the Email Server created previously.
The FortiAnalyzer Configuration is now complete.

**IBM RESILIENT CONFIGURATION**

This guide assumes that the IBM Resilient IRHub is already installed and configured.

Refer to Resilient Email Connector Config Guide v2.x for more details.

Install the Email Connector package using the following command, where `<version>` is the run file version.

```
Last login: Tue Jun  5 16:21:27 2018 from 10.101.32.254
-bash-4.2$ sudo rpm -i irhub-mail-<version>.rpm
```
If using the IMAP protocol, run the IMAP script to configure the email account to monitor by entering the following command and following the prompts.

```
Last login: Tue Jun 5 16:21:27 2018 from 10.101.32.254
-bash-4.2$ sudo irhub-imap-cfg
```

As prompted, enter the following information:
- IMAP mail server host name; for example, mail.example.com
- Trust the certificate (only prompted if the certificate is untrusted)
- IMAP username; for example, resilient@example.com
- IMAP user password

The script concludes by stating the location of the configuration file. For example:

```
Selecting mailbox INBOX OK
IMAP configuration settings were written to
/usr/share/irhub/etc/irhub.mail.cfg
```

If using the EWS protocol, run the EWS script to configure the email account to monitor by entering the following command and following the prompts.

```
Last login: Tue Jun 5 16:21:27 2018 from 10.101.32.254
-bash-4.2$ sudo irhub-ews-cfg
```

As prompted, enter the following information:
- EWS endpoint; for example, https://mail.example.com/ews/exchange.asmx
- Trust the certificate (only prompted if the certificate is untrusted)
- EWS username; for example, resilient@example.com
- EWS user password

**NOTE:** it must be in email format. Domain\Username format does not work.
- EWS user password

The EWS script automatically sets the mail_protocol property to EWS. If using the EWS script to make changes after the initial installation, make sure to restart the IRHub for the updates to take effect.

The script concludes by stating the location of the configuration file. For example:

```
Using the following settings:
Endpoint = https://mail.example.com/ews/exchange.asmx, Mailbox = Inbox
EWS configuration settings were written to
/usr/share/irhub/etc/irhub.mail.cfg
```
Restart IRHub as follows:

```
Last login: Tue Jun 5 16:21:27 2018 from 10.101.32.254
-bash-4.2$ sudo systemctl restart irhub
[sudo] password for resadmin:
-bash-4.2$
```

At this point FortiAnalyzer will send an Email Alert to Resilient when there is a failed Admin logon via SSH.
You can test this by making several failed authentication attempts to the FortiAnalyzer CLI:

```
Last login: Wed Jun 6 10:59:07 on ttys000
kgallagher-mac:~ kgallagher$ ssh admin@10.101.32.67
kgallagher-mac:~ kgallagher$
```

Now login to the Resilient GUI and check List Incidents. It should look like the image below:
Notice that the Incident Name is populated by the Email Subject and a description of the Incident is included.

Click on an Incident Name to view more details.

Notice that an ID Number is automatically assigned to the Incident.

The Incident indicates which device the Incident came from, in this case FAZ-VM0000101910.

The full Log message is also included in the Incident.

**SUMMARY**

Fortinet and IBM Resilient