Setup Guide | Forcepoint Email Security in Microsoft Azure

Before you begin...

1. Verify Requirements
   - A Microsoft Azure account (activated)
   - A running SQL Server instance with connectivity to an existing Azure virtual network (if you are installing version 8.5 or only installing email appliances in Azure; otherwise, a SQL Server instance in Azure will be configured during step 2)
   - Forcepoint Security Manager running on-premises with connectivity to an existing Azure virtual network (if you are installing version 8.5 or only installing email appliances in Azure)
   - Forcepoint Security Manager upgraded to version 8.5.3
   - A virtual network in Azure with connectivity to on-premises resources through a site-to-site VPN (if you are installing version 8.5 or only installing email appliances in Azure)
   - Microsoft Office 365 with Outlook

2. Deploy Virtual Appliance and Machine in Azure
   b. Locate Forcepoint Email Security in the Azure Marketplace.
   c. Create a VA for Forcepoint Email Security and a VM for Forcepoint Security Manager and SQL Server in the Azure cloud. (FSM and SQL in Azure are only supported for v8.5.3).

3. Configure DNS Name and Static IP Address in Azure
   a. In Azure, add a static public IP address for your email VA (or your load balancer, if using a cluster).
   b. In Azure, add a DNS name for all public IP addresses.

4. Configure the Forcepoint Email Security VA
   a. Log into the appliance CLI.
   b. Configure time zone.

5. Install Forcepoint Security Manager Components (v8.5 only)
   a. Run the Forcepoint Security Manager unified installer on your management server.
   b. Select Install.
   c. Complete the Forcepoint Email Security installation wizard.

6. Configure Virtual Appliance
   - Forcepoint Email Security
     a. Log onto the Forcepoint Security Manager and select the Email tab.
     b. Supply the FQDN for the virtual appliance.
     c. Configure protected domains and SMTP servers.
     d. Configure an administrator email address for notifications.
     e. Register all necessary appliances with the Forcepoint DLP module.
   - Data Security manager
     f. Select the Data tab in the Forcepoint Security Manager.
     g. Add the network email destination to policies that should be used for this appliance.
     h. Click Deploy.

7. Configure Exchange Online
   a. Log onto Office 365 and click Exchange.
   b. Add a new mail flow connector that routes mail according to your deployment:
      - From Office 365 to a Cooperative Partner or Organizer
      - From a Cooperative Partner or Organizer to Office 365
   c. Specify the IP address of the Forcepoint Email Security virtual appliance as the route machine.
Virtual appliance configuration information:

- Azure Subscription ID
- Azure region
- Email VA name
- Email VA user name and password
- Security Manager VM name
- Security Manager VM user name and password
- Resource group (ForcepointResource by default)
- VNet
- Subnet
- Public IP address
- Network security group

Support and Resources:  Forcepoint

Online Support and Contact Information:  support.forcepoint.com