Installing Forcepoint Web Security in Microsoft Azure

Installation | Forcepoint Web Security | Version 8.5.x

Forcepoint Web Security deployed in a Microsoft Azure environment allows you to develop and enforce policies to protect your network. Together, a series of web protection components provide security for web-based transactions, as well as management, user identification, alerting, reporting, and troubleshooting capabilities. The Content Gateway component performs advanced content analysis precisely when it is needed—as the content flows through the proxy. The results of analysis are used by Forcepoint Web Security to protect you from malicious content and apply your Acceptable Use Policy (AUP).

In order to deploy Forcepoint Web Security in Azure, a virtual network must be created and configured with subnets, each of which should have its own network security group. The virtual network must also be configured with a resource for terminating a site-to-site Virtual Private Network (VPN).

Create Azure virtual machines on which the Web Security components will be installed. The Azure installation process then mirrors the process used for software deployments.

- System requirements
- Forcepoint Web Security Administrator Help

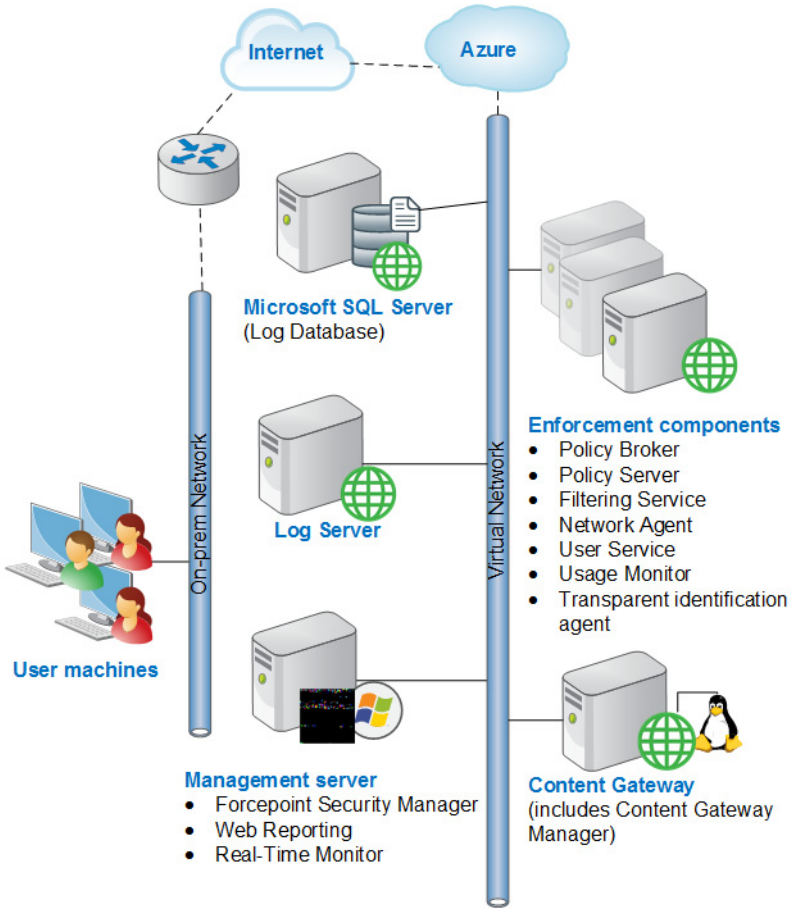
Note

Components that are Windows-only must be installed on a Windows Azure VM using a supported version of Microsoft Windows. Similarly Linux-only components must be installed on a Linux Azure VM with a supported version of Red Hat Enterprise Linux.Refer to the Product Matrix for the list of supported operating systems.

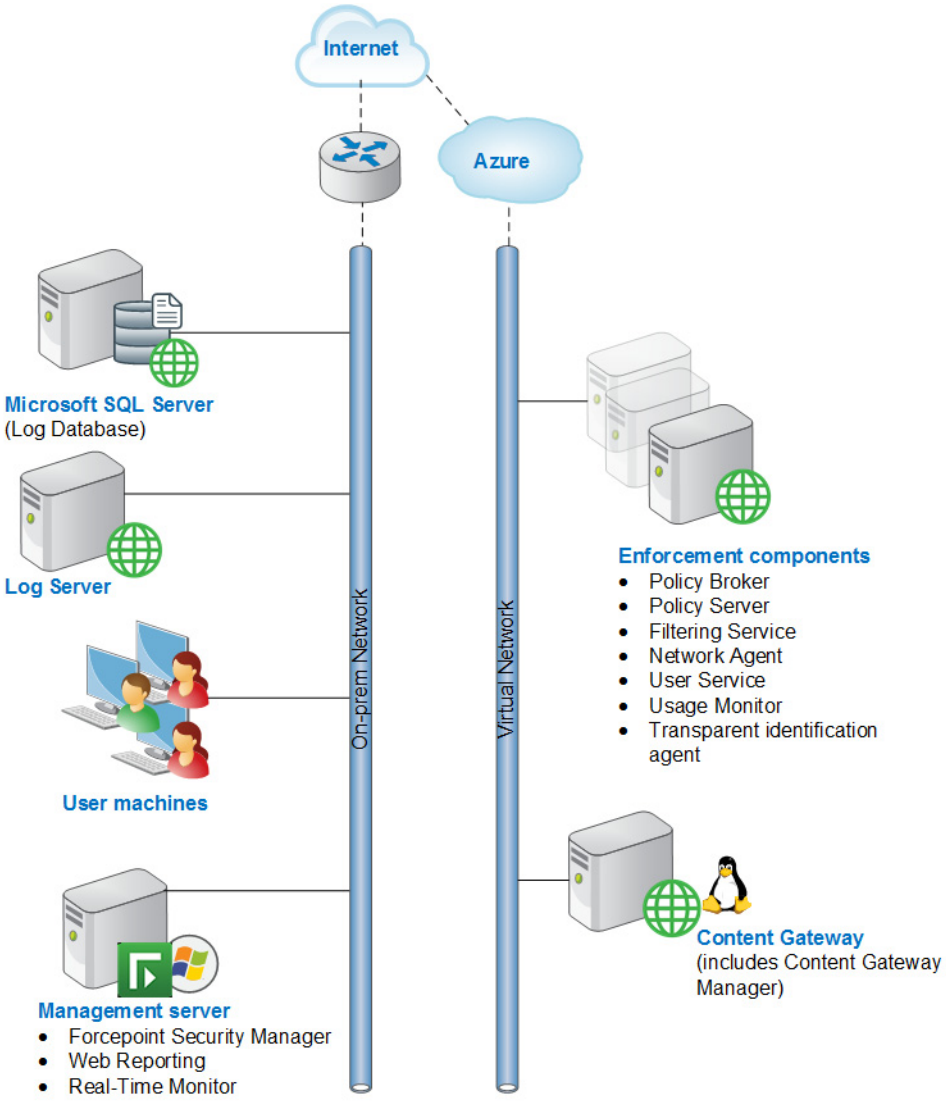
Forcepoint Web Security in Azure: Deployment Scenarios

Web protection in Azure can be deployed in several ways.

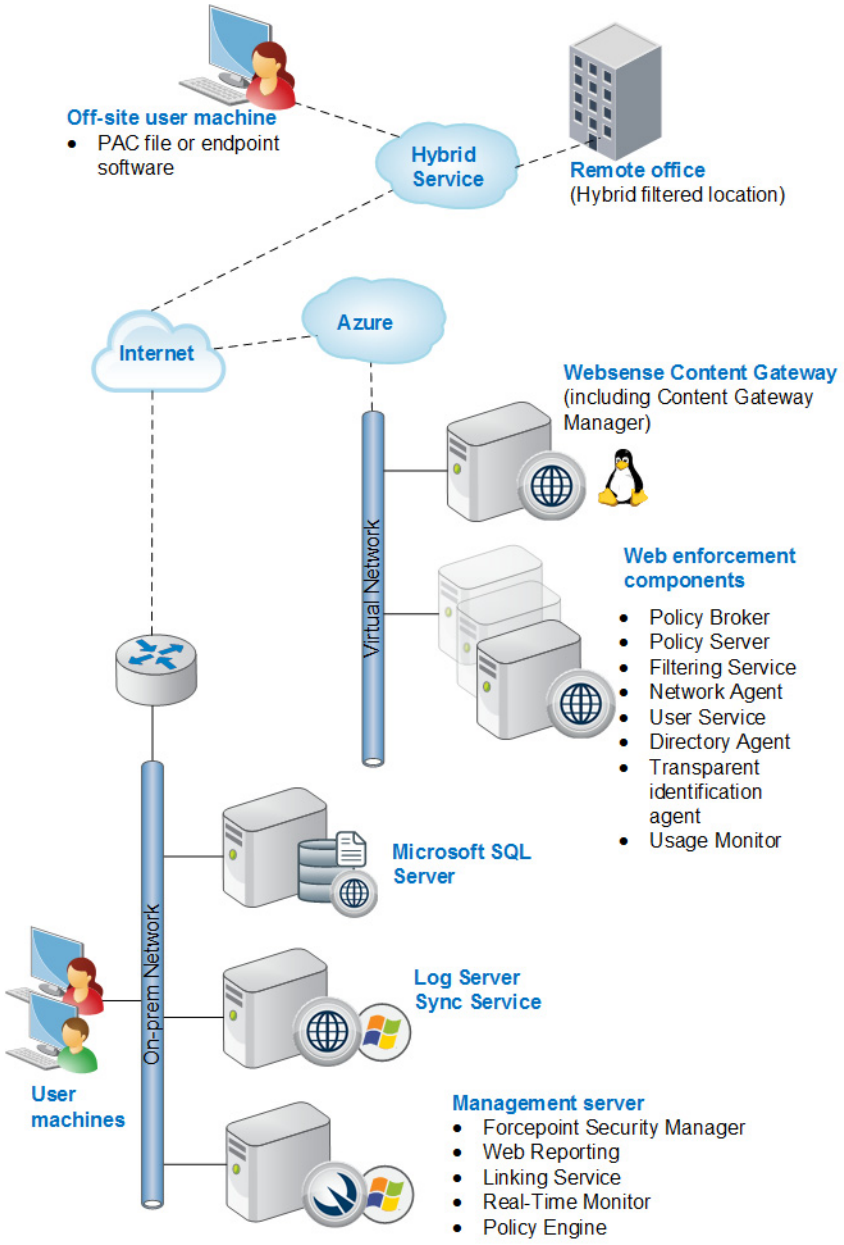
- Forcepoint URL Filtering with dedicated machines for the Log Database, Log Server, a Management Server, and all other components.



- Forcepoint Security Manager with LogServer and the Log Database installed on-premises, and all other components on Azure virtual machines.



- Forcepoint Web Security in a hybrid deployment.



Requirements

- A Microsoft Azure account (activated)
- A virtual network and subnet in Azure with connectivity to on-premises resources through a site-to-site VPN

- Resources installed on-premises.

  There are no components that must be installed on-premises. However, if an Azure VM is used to support the Log Database, a supported version of Microsoft SQL Server must be installed. Microsoft Azure SQL Database is not supported.
- Azure virtual machines must be configured to support everything that an on-premises installation would be required to support. For example:
  - The virtual machine must have a static IP address.
  - Local domain rights are needed to install the product.
  - By default, the ports listed on the Web Protection tab of this Excel spreadsheet must be open.
  - The same system requirements must be met.
- Traffic must be explicitly routed to Content Gateway by configuring the client's Internet browser. See Content Gateway Help for details.

  Transparent redirection of user traffic is not supported.

Recommendations:

To speed up user authentication, a directory service that mirrors the on-premises directory service should be installed on an Azure virtual machine.

Deployment steps

Use the following steps to deploy Forcepoint Web Security in Azure:

1. Create a site-to-site VPN.

   See Microsoft documentation for more information.
2. Log on to the Azure Marketplace, https://portal.azure.com/, and click **Create a resource**.
3. Create virtual machines to support installation of Web Security

   This step should be take after a plan for how your web protection solution will be deployed. Create as many VMs as needed to accommodate all of the components your plan to install.
4. Determine which components will reside on each machine, either virtual or on-premises, and begin the installation process.

   Follow the instructions found in this document, paying strict attention to the order in which components must be installed.