FORCEPOINT
POWERED BY Raytheon

Forcepoint Appliances Getting Started Guide

V Series, X Series, & Virtual Appliances

v8.4.x

Published 2018
Printed in the United States and Ireland

D230317840

Trademarks

Contents

Topic 1 **Forcepoint Appliances 1**

Supported software 2
- Forcepoint Email Security 2
- Forcepoint Web Security 2
- Forcepoint URL Filtering 2
- Forcepoint DLP 3

Appliance platforms 4
- V Series 4
- X Series 4
- Forcepoint Virtual Appliances 5

Features 6
- Platform hardening 6
- Command-line interface 6
- Forcepoint Security Appliance Manager 7
- Custom appliance user account management 7
- Forcepoint appliance platform API 7
- Stacking module on X10G 7
- 10GBe PCI NIC on V10K 7

Deployment 8

Configuration and management 8

Documentation 8

Topic 2 **Deploying Forcepoint Appliances 11**

Deployment planning 11

Deployment big picture 13
- Required off-appliance components 14
- Web protection deployments 15
- Forcepoint Email Security deployments 20

Deployment activity summary 21

Forcepoint appliance installation summary 21

Topic 3 **V Series Hardware Setup 23**

V10000 hardware setup 24
- V10000 with Forcepoint Web Security 24
- V10000 with Forcepoint Email Security 24

V5000 hardware setup 25

Using the iDRAC 26

Connecting directly to the appliance 27
Topic 4 **X Series Hardware Setup 29**
X10G hardware setup 29
Receiving and racking the hardware 30
Unloading at your shipping dock 30
X10G Quick Start poster 31
Security blade slots 31
iDRAC and interface IP address planning 32
X10G chassis cabling 33
Power on 35
Set up the CMC IP Address 36
Assigning blade slot iDRAC addresses 37
iDRAC Virtual Console 38
Topic 5 **Forcepoint Virtual Appliance Setup 39**
Creating a Forcepoint ESXi VMware virtual appliance 39
Virtual appliance creation summary 39
Creating the virtual machine 40
Topic 6 **Firstboot Wizard 41**
The firstboot wizard (initial command-line configuration) 41
Gather data for firstboot 42
Run firstboot 44
Topic 7 **Configure Appliances (post-firstboot) 47**
SSH access to the CLI 47
Verify firstboot configuration settings 48
Configuration basics 48
Appliance management interface (C) 49
System time and time synchronization with Forcepoint servers 49
Add an appliance description 50
Establish a filestore 51
Set an email address for password recovery 51
Configure additional network interfaces 52
Support for IPv6 52
Appliance management interface (C) 53
Content Gateway (web proxy) interfaces (P1 and P2) 53
Web protection: Network Agent interface (N) 55
Forcepoint Email Security interfaces (E1 and E2, or P1 and P2) 56
Interface bonding 58
Configure routes 59
Static routes 59
Component routes 60

SNMP polling and alerting 60
SNMP traps 61
Topic 8 **Installation of Off-Appliance Components 63**

1 Forcepoint Appliances

Getting Started | Forcepoint Appliances | Version 8.4.x

Related topics:

- *Supported software*, page 2
- *Appliance platforms*, page 4
- *Features*, page 6
- *Deployment*, page 8
- *Configuration and management*, page 8
- *Documentation*

Forcepoint appliances are purpose-built machines for core components of Forcepoint DLP, Forcepoint Email Security, Forcepoint Web Security, and Forcepoint URL Filtering. Forcepoint appliances are security-hardened (see *Platform hardening* and optimized for performance, reliability, and ease of use.

This guide provides general information about Forcepoint appliances, as well as in-depth information about deploying Forcepoint appliances with Forcepoint Email Security, Forcepoint Web Security, and Forcepoint URL Filtering.

- For detailed information about Forcepoint DLP on Forcepoint appliances, including Forcepoint DLP Cloud Email (Microsoft Azure), see the Forcepoint DLP section of the Forcepoint documentation page.
- For detailed information about Forcepoint Web Security Cloud with I Series appliance, see the Forcepoint I Series Appliance section of the Forcepoint Documentation page.

Supported software

Forcepoint appliances support:

- *Forcepoint Email Security* with integrated data loss prevention
- *Forcepoint Web Security* with integrated data loss prevention
- *Forcepoint URL Filtering* — V5000 and VMware virtual appliances
- *Forcepoint DLP*
  - Protector
  - Mobile Agent
  - Forcepoint DLP Cloud Email (Microsoft Azure)

Forcepoint Email Security

Forcepoint Email Security provides comprehensive on-premises email security. Each message is processed by a robust set of analytics to prevent infected and other unwanted email from being delivered. Domain and IP address based message routing ensures reliable, accurate delivery of email. The optional Forcepoint Email Security Hybrid Module adds support for pre-filtering messages in the cloud. For more information, see Deploying Email Protection Solutions in the Forcepoint Deployment and Installation Center.

Forcepoint Web Security

Forcepoint Web Security provides protection against malware entering the network via Web channels, such as HTTP, HTTPS, and FTP.

Forcepoint Web Security:

- Performs real-time content analysis to discover malware and hidden threats.
- Can monitor traffic that uses any of more than 100 protocols.
- Provides highly-granular and flexible control of Internet access to enforce the precise requirements of an organization's Acceptable Use Policy (AUP)
- Can be used in combination with Forcepoint Web Security Cloud to provide cloud-hosted Web protection to users working both within the organization's network and outside the network—wherever the user is accessing the Internet.

For more information, see Deploying Web Protection Solutions in the Forcepoint Deployment and Installation Center.

Forcepoint URL Filtering

Forcepoint URL Filtering provides granular and flexible control of Internet access to enforce the precise requirements of an organization's Acceptable Use Policy (AUP). Features include:

- Granular Web security policy controls
- More than 120 Web security and content categories
- Custom allow/deny filters enforced 24/7 or adjusted by time and day
- Time quotas with multiple authentication options for users and groups
- Granular user behavior analysis reporting with more than 60 predefined reports, and support for role-based access

Forcepoint DLP

Important
Information about Forcepoint DLP appliances is not included in this guide. See the Forcepoint DLP section of the Forcepoint Documentation page.

Forcepoint DLP protects organizations from information leaks and data loss. It can operate alone in the network, or can be paired with Forcepoint Web Security, Forcepoint Email Security, or both.

Forcepoint DLP Network prevents data loss through email and over Web channels. It includes Forcepoint DLP Cloud Email, deployed in Microsoft Azure. It provides DLP policy enforcement for Microsoft Exchange Online.

The protector appliance intercepts and analyzes traffic on a variety of channels, such as email, HTTP, and FTP. (HTTP traffic is monitored but not enforced.)

The mobile agent appliance can be configured to secure email content that is synchronized to a user's mobile devices via Exchange ActiveSync. This includes content in email messages, calendar events, and tasks.

Forcepoint DLP includes an analytics engine that identifies and ranks high-risk incidents. It consumes incidents generated by DLP policies and reports on those with the highest data loss or data theft risk score.

Forcepoint Data Discovery is used to learn the location of sensitive data within on-premises data centers and cloud hosted applications. It can be configured to scan data on file servers, email servers, databases, and content collaboration applications.

Forcepoint DLP Endpoint prevents data loss over endpoint channels such as removable storage devices, mobile devices, browser uploads, email clients, and applications. It can also discover and remediate sensitive data stored on laptop and desktop systems.

For more information, see the Forcepoint DLP Deployment Guide (PDF).

Appliance platforms

Forcepoint appliance platforms include:

- V Series hardware
- X Series hardware
- VMware ESXi virtual appliance
- Microsoft Azure cloud-hosted appliance

V Series

1 rack-unit form factor

See the V-Series Appliance datasheet (PDF) for specifications of the current model.

Models supported with version 8.4:

- V10000 G4 (Forcepoint Web Security, Forcepoint Email Security (V1000 & V5000)
- V10000 G3

All V10000 models support Forcepoint Web Security or Forcepoint Email Security

- V5000 G4
- V5000 G3
- V5000 G2R2

All V5000 models support Forcepoint Web Security, Forcepoint URL Filtering, or Forcepoint Email Security

V Series Hardware Setup

X Series

10 rack-unit form factor; chassis hosts up to 16 X10G blade servers

See the X-Series Appliance datasheet (PDF) for specifications of the current model.

Models supported with version 8.4:

- X10G G2 blade server
- X10G G1 blade server

All X10G models support Forcepoint Web Security or Forcepoint Email Security

X Series Hardware Setup

Forcepoint Virtual Appliances

ESXi VMware

VMware virtual appliances are certified with ESXi versions 5.5, 6.0, and 6.5.

Supported Forcepoint solutions

- Forcepoint Email Security
- Forcepoint Web Security

Forcepoint Email Security VM specification

The install OVA creates a virtual machine with the following specifications:

- 6 CPU cores
- 12 GB RAM
- 1 - 225 GB disk
- 1 - 100 GB disk
- 4 E1000 virtual network interfaces (1 reserved port)

Important

These resources must be maintained as specified.

When Forcepoint security software starts, if the resources do not match the specification, the application containers do not start. In the CLI, a persistent message displays indicating that the resources have been modified.

Network interfaces

All VMware virtual appliances come with 4 virtual Ethernet interfaces.

C — Supports appliance management communication

P1, **P2** — Support MTA traffic

N — Reserved

Forcepoint Web Security VM specification

The install OVA creates a virtual machine with the following specifications:

- 6 CPU cores
- 12 GB RAM
- 1 - 129 GB disk
- 1 - 128 GB disk

- 4 E1000 virtual network interfaces (1 reserved port)

> **Important**
> These resources must be maintained as specified.
>
> When Forcepoint security software starts, if the resources do not match the specification, the application containers do not start. In the CLI, a persistent message displays indicating that the resources have been modified.

Network interfaces

All VMware virtual appliances come with 4 virtual Ethernet interfaces.

C — Supports appliance management communication

P1, **P2** — Support Content Gateway web proxy traffic

N — Reserved; Network Agent and the Content Gateway decryption mirror port feature are not supported on VMware virtual appliances.

Forcepoint Virtual Appliance Setup

Decryption Port Mirror Expansion

In X Series appliances with the switch configuration port installed, the decryption mirror port expansion allows you to use the CLI or the API to enable the N interface as an SSL mirror port rather than a Network Agent port.

Features

Platform hardening

These measures harden all Forcepoint V Series, X Series, and Virtual Appliances:

- CentOS 7.2 operating system -- Base operating system and Forcepoint Email Security container
- CentOS 6.8 operating system -- Web protection containers (Web, Proxy, Network Agent)
- SELinux enabled (not enforcing)
- Apache Tomcat removed

Command-line interface

All Forcepoint appliances share a common command-line interface (CLI) that supports all appliance management functions, including monitor, configuration, and troubleshooting.

After initial appliance configuration, performed with the **firstboot** wizard, the CLI can be accessed via SSH and a terminal emulator such as PuTTY. In addition, V Series and X Series appliances can access the CLI through the Virtual Console feature of the integrated Dell Remote Access Controller (iDRAC), or by attaching a keyboard and monitor directly to the appliance. On VMware virtual appliances, the CLI can also be accessed in the vSphere Client.

The CLI has 3 modes: **view**, **config**, and **diagnose**.

For more information, see the Forcepoint Appliances CLI guide.

Forcepoint Security Appliance Manager

The Forcepoint Security Appliance Manager is a centralized management console for all of your Forcepoint V Series, X Series, and Virtual Appliances.

For more information, see the Forcepoint Security Appliance Manager guide.

Custom appliance user account management

Custom appliance accounts can be created, allowing for more accurate user management and audit logging. Audit users can view configuration information; admin users can view and edit configuration information, and super admin users can also create, delete, and update user accounts. Multiple account instances can be created for specific roles.

Forcepoint appliance platform API

All configuration, management, and troubleshooting functions are supported by a REST API that is used by all Forcepoint appliance platforms and tools. The CLI uses the REST API, as does the Forcepoint Security Appliance Manager.

Basic and Certificate Authentication are supported in the appliance API.

Stacking module on X10G

The Dell stacking module is supported on the X10G appliance as a hardware add-on. This will allow X10G deployment with the same switch-level High Availability (HA) compliance. For installation instructions, see the X10G Switch Stack Module Installation Guide.

10GBe PCI NIC on V10K

The Dell 10GBe PCI NIC is supported on the V10K appliance as a hardware add-on, allowing the V10K to be deployed into a pure fiber network. For installation instructions, see the V10K 10GBe PCI NIC Installation Guide.

Deployment

Forcepoint security deployments vary from small to very-large. In deployments that include Forcepoint appliances, several off-appliance servers are used to host the Forcepoint Security Manager and related infrastructure, the Log Server, and an Enterprise installation of Microsoft SQL Server.

Deployment is discussed in detail in *Deploying Forcepoint Appliances*, page 11.

Configuration and management

Forcepoint appliances are configured and managed with the command-line interface (CLI), the Forcepoint Security Appliance Manager, and the appliance API.

Configuration and management activities generally include:

- Setting, synchronizing, and monitoring the system time and date
- Configuring network interfaces
- Defining a filestore location and filestore name alias
- Configuring the STP bridge, if used (X Series only)
- Defining static routes, as needed
- Optionally, enabling and configuring SNMP traps
- Monitoring system performance
- Reviewing system log files
- Installing upgrades and hotfixes
- Scheduling and performing backups
- Enabling and disabling logon accounts, as needed
- Running system diagnostics, as needed

For detailed information, see the Forcepoint Appliances CLI Guide.

Documentation

Forcepoint appliance documentation includes:

- This guide — Forcepoint Appliances Getting Started

- Forcepoint Appliances Release Notes
- Forcepoint Appliances CLI Guide
- Forcepoint V Series, X Series, and Virtual Appliance Upgrade Guide
- V Series Upgrade Guide
- V Series: Upgrading DUAL MODE Appliances to Version 8.4
- V Series Quick Start Posters
- X Series Upgrade Guide
- X Series Quick Start Poster
- X Series Switch Configuration Guide
- X Series Fiber Optics Kit

All Forcepoint documentation, including documents specific to Forcepoint Email Security, Forcepoint Web Security, Forcepoint URL Filtering, and Forcepoint Security Manager can be accessed at support.forcepoint.com/documentation.

See, also, the Forcepoint knowledge base. Go to www.support.forcepoint.com and use Search.

2 Deploying Forcepoint Appliances

Getting Started Guide | Deploying Forcepoint Appliances | Version 8.4.x

Related topics:

- *Deployment planning*, page 11
- *Deployment big picture*, page 13
- *Deployment activity summary*, page 21
- *Forcepoint appliance installation summary*, page 21

This guide provides general information about Forcepoint appliances, as well as in-depth information about deploying Forcepoint appliances with Forcepoint Email Security, Forcepoint Web Security, and Forcepoint URL Filtering.

- For detailed information about Forcepoint DLP on Forcepoint appliances, including Forcepoint DLP Cloud Email, see the Forcepoint DLP section of the Forcepoint documentation page.
- For detailed information about Forcepoint Web Security Cloud with I Series appliance, see the Forcepoint I Series Appliance section of the Forcepoint Documentation page.

Important
Before deploying Forcepoint technologies, work with your Forcepoint distributor and Forcepoint Sales Engineer to create a deployment plan. A vetted deployment plan is the best preparation for a trouble-free deployment that delivers the results you expect.

Deployment planning

A detailed deployment plan is essential to achieving an efficient, trouble-free deployment. If the deployment is large or complex, engage your Forcepoint distributor and Forcepoint Sales Engineer for assistance.

A complete deployment plan includes:

1. **A list of Forcepoint security technologies to be deployed**, their components, where the components are installed, and their requirements and dependencies, including version compatibility with other components, host operating system, and third-party software components.
2. **A careful estimate of the computer and network resources needed** to meet your performance requirements, and that meet the requirements of the technologies to be deployed.
3. **A plan for the location of physical equipment** and its placement in the network, including subnetting and reserved IP addresses.
4. **An understanding of point-to-point network port requirements**, firewall rules, routing, and other network configuration provisions.
5. **A configuration plan for your Forcepoint security solutions** (web, email, DLP, and end points) that defines needed policies and rules.
6. **If using X Series equipment**, special arrangements need to be made for taking delivery of the hardware. Due to its size and weight, X Series has special requirements. See *Receiving and racking the hardware*, page 30, in this guide.

Use the following resources in the preparation of your deployment plan.

- This guide
- The Forcepoint Deployment and Installation Center, including:
  - Deploying Email Protection Solutions
  - Deploying Web Protection Solutions
  - Planning Forcepoint DLP Deployment
  - Forcepoint system requirements
  - Review the list of Default ports for on-premises Forcepoint solutions
- The Forcepoint appliances documentation set, which can be accessed in the Forcepoint Appliances section of the Forcepoint Documentation page. Locate the platform of interest (e.g., Forcepoint V10000 Appliance) and select the version you are deploying. Of particular interest are:
  - This guide
  - Hardware setup posters
  - X Series Switch Configuration Guide (X Series deployments only)
  - Release notes

Deployment big picture

In this section:

- *Required off-appliance components*, page 14
- *Web protection deployments*, page 15
- *Forcepoint Email Security deployments*, page 20

Forcepoint deployments can include any or all of these Forcepoint solutions:

- Forcepoint DLP
- Forcepoint Web Security, with or without hybrid cloud web protection services
- Forcepoint Email Security, with or without hybrid cloud email protection services
- Forcepoint Endpoint

Important

Forcepoint appliances are one component of a complete Forcepoint security solution.

When you are ready to begin deployment, be sure to start with the installation guides for your Forcepoint security solutions. Those guides link to this guide for appliance setup and initial configuration activities.

See these topics in the Forcepoint Deployment and Installation Center to become familiar with the details of Forcepoint deployments.

- Deployment planning for Forcepoint solutions
- System requirements
- Default ports for on-premises Forcepoint solutions

Forcepoint Web Security and Forcepoint URL Filtering

- Deploying Web Protection Solutions
- Deploying Forcepoint Web Security in a distributed enterprise

Forcepoint Email Security

- Deploying Email Protection Solutions

Forcepoint DLP

- Planning Forcepoint DLP Deployment
- Installing Forcepoint DLP Agents
- Integrating Forcepoint DLP with Existing Infrastructure
- Scaling Forcepoint DLP

Required off-appliance components

All deployments include several off-appliance servers that host additional components.

- A Windows Server to host the *Forcepoint infrastructure*, including the *Forcepoint Security Manager*. The Forcepoint Security Manager supports configuration and management of your Forcepoint solutions. This server is sometimes referred to as the Forcepoint management server.
- Web protection solutions locate several additional components on the Forcepoint management server, or on a separate Windows or Linux server.
- Web and email deployments require a Windows Server to host the Log Server service. Log Server manages the handling of log data with the SQL Server database and with Forcepoint reporting services.
- Data, web, and email solutions require a Windows Server to host an instance of Microsoft SQL Server. SQL Server supports the Forcepoint Log Database.
- Forcepoint Email Security deployments require a mail server.

For server specifications, see System requirements in the Deployment and Installation Center.

Important
All components in the deployment, including those running off-appliance, must run the same version of Forcepoint software.

Forcepoint infrastructure

Forcepoint security infrastructure is made up of many components, including a web-browser-based graphical user interface and logging and reporting components. Services include:

- Forcepoint Security Manager
- Forcepoint Central Access
- Forcepoint Settings Database
- Forcepoint Reporting Database (if using SQL Server 2008 R2 Express)

Note
SQL Server 2008 R2 Express should be used only in evaluation environments.

Full SQL Server should be used in all production environments.

Forcepoint Security Manager

Forcepoint Security Manager is the web-browser-based, graphical management component that provides configuration, policy management, and reporting functions.

It includes one or more of the following modules, depending on your subscription: Web, Data (DLP), and Email. Each module is used to configure and manage its respective features.

Log Server

Instances of Log Server, one for web security deployments and one for email security deployments, receive information about Internet and email activity and process the information into their respective Log Database.

Because record processing is resource-intensive, Log Server is installed on its own Windows Server and should not run on the same machine as other resource-sensitive components, such as Filtering Service, the Forcepoint management server, or the SQL Server host.

Log Server cannot be installed on an appliance.

Log database

Web and email products require Microsoft SQL Server to host the reporting database, called the Log Database. The Web Log Database and the Email Log Database can be hosted by the same database engine instance. Information stored in the Log Database is used to create reports.

Before you install Web or Email Log Server, SQL Server must be installed and running on a machine in your network. SQL Server must be obtained separately; it is not included with your subscription.

Web protection deployments

Web protection deployments include Forcepoint Web Security and Forcepoint URL Filtering.

Important

- Web protection deployments can use a mix of Forcepoint platforms — V Series, X Series, Virtual Appliances, and standalone Windows and Linux servers.

Policy source

In a web protection deployment, there is a **policy source** machine that hosts 2 components that do not run on any other server or appliance: **Policy Database** and

Policy Broker. One of the first deployment decisions that must be made is the location of the **policy source** machine.

Important

- Deployments that include installations of Policy Server on standalone Windows or Linux servers and on Forcepoint appliances, must locate the policy source on a Windows or Linux server, and not on a Forcepoint appliance.
- Deployments that configure Policy Broker Replication must locate the primary and replica Policy Broker instances on Windows or Linux servers.

All machines running Web protection components connect to the policy source machine to get up-to-date policy information. Your primary instance of **Policy Server** also runs on the policy source machine.

Most sites install the policy source on a Windows server (off-appliance). An alternative is to configure a V Series or X Series appliance (located in Slot-1). The **policy mode** of remaining appliances is chosen during each appliance's firstboot. Here's how it works:

1. The policy source machine is set up, either off-appliance or on-appliance.
2. When other appliances go through firstboot, the policy mode is set to either **User directory and filtering** mode or **Filtering** only mode.

If the policy source is located off-appliance, you have the option to configure replicated policy source servers. See Managing Policy Broker Replication.

User directory and filtering

A **User directory and filtering** appliance is a lightweight version of the policy source machine.

Whenever you make a policy change, that change is immediately updated on the policy source appliance. The change is pushed out to user directory and filtering appliances within 30 seconds.

If the connection with the policy source machine is interrupted, user directory and filtering appliances can continue handling traffic for as long as 14 days. So even if a network connection is poor or is lost, traffic processing continues as expected.

A user directory and filtering appliance is configured to point to the full policy source for updates.

A **User directory and filtering** appliance runs:

- Policy Server
- User Service
- Usage Monitor

- Filtering Service
- Control Service
- Directory Agent
- Content Gateway module (Forcepoint Web Security only)

Filtering only

A **Filtering only** appliance is configured to point to a Policy Server. This works best when the appliance is close to the Policy Server and on the same network.

These appliances require a continual connection to the centralized Policy Server, not only to stay current, but also to continue handling traffic. If the connection to the Policy Server becomes unavailable for any reason, traffic on a filtering only appliance will continue to be handled for up to 3 hours.

A **Filtering only** appliance does not run Policy Server. It runs only:

- Filtering Service
- Control Service
- Content Gateway module (Forcepoint Web Security only)

Content Gateway (web proxy)

Content Gateway is a high-performance web proxy. It is installed on every Forcepoint Web Security appliance. In addition to providing core web proxy request handling and page caching (optional), it applies Forcepoint real-time threat analytics and website classification to protect the network from attacks and malicious and undesirable content.

Content Gateway includes:

- Real-time HTTP, HTTPS, and FTP content analysis
- Real-time categorization of websites
- Enterprise web caching (optional)
- A web-based graphical user interface for configuring, monitoring, and managing Content Gateway.

Once installed and running, the Content Gateway Manager is accessed by entering:

```
https://<Appliance C interface IP address>:8081
```

Log on with “admin” and the password established during firstboot.

Table of Web security components

Following is a brief description of Forcepoint web protections components.

For component limits and rations, see Deploying core web protection components in the Forcepoint Technical Library.

The individual components required for these modes are automatically enabled when firstboot completes. You do not need to choose components individually.

Component	Description
Policy Database	Stores Forcepoint software settings and policy information. Installed automatically with Policy Broker. Runs on the **policy source** machine only. Typically installed on a Windows server.
Policy Broker	Manages requests from Forcepoint components for policy and general configuration information. Runs on the **policy source** machine only. Typically installed on Windows server.
Policy Server	Can run on any web appliance. The primary copy runs on the **policy source** machine. ● Identifies and tracks the location and status of other Forcepoint components. ● Stores configuration information specific to a single Policy Server instance. ● Communicates configuration data to Filtering Service, for use in handling Internet requests. Policy Server settings are configured in the Web Security module of the Security Manager. Policy and most configuration settings are shared among all Policy Servers that share a Policy Database.
Filtering Service	Can run on any web appliance. Provides Internet traffic management in conjunction with Network Agent or a third-party integration product. When a user requests a site, Filtering Service receives the request and determines which policy applies. ● Filtering Service must be running for Internet requests to be handled and logged. ● Each Filtering Service instance downloads its own copy of the Forcepoint Master Database. Configure enforcement policies and Filtering Service behavior in the Web Security module of the Security Manager.
Network Agent	Can be deployed on V Series appliances and Windows and Linux servers. ● Enhances security and logging functions ● Enables non-HTTP and non-HTTPS protocol management
Master Database	● Includes more than 36 million websites, sorted into more than 95 categories and subcategories ● Contains more than 100 non-HTTP protocol definitions for use in managing protocols After all modules are set up, download the Forcepoint Master Database to activate Internet management, and schedule automatic updates. If the Master Database is more than 2 weeks old, no traffic management occurs.

Component	Description
Forcepoint Web Security module of the Forcepoint Security Manager	Runs on a Windows server. Serves as the configuration, management, and reporting interface for Forcepoint software. Use the Web Security module of the Security Manager to define and customize Internet access policies, configure Forcepoint software components, report on Internet activity, and more. The Web Security module of the Security Manager is made up of the following services: ● Web Security ● Web Reporting Tools ● Explorer Report Scheduler ● Information Service for Explorer ● Reporter Scheduler ● Real-Time Monitor
Usage Monitor	Can run on any appliance. ● Enables alerting based on Internet usage. ● Provides Internet usage information to Real-Time Monitor. Usage Monitor tracks URL category access (shown in Real-Time Monitor) and protocol access, and generates alert messages according to the alerting behavior you have configured.
Content Gateway	Runs on every Forcepoint Web Security appliance. ● Provides a robust proxy and cache platform. ● Can analyze the content of websites and files in real time to categorize previously uncategorized sites. ● Analyzes HTML code to find security threats. ● Inspects file content to assign a threat category (for example, viruses, Trojan horses, or worms).

Web protection Default policy

Forcepoint Web Security and Forcepoint URL Filtering include a **Default** policy that is in effect 24 hours a day, 7 days a week. Initially, this policy monitors Internet traffic without blocking. When you first install a web protection solution, the Default policy applies to everyone on the network. To customize the policy, use the Web Security module of the Forcepoint Security Manager and its embedded Help system.

Forcepoint Email Security deployments

Important

If you deploy Forcepoint Email Security on an X10G chassis that also hosts Forcepoint Web Security blades, you must choose a location for and configure the Forcepoint Web Security **policy source** (Policy Broker/ Policy Database) machine before configuring any other web or email appliances. See *Policy source*, page 15, for details.

Email components

The following services run on Forcepoint Email Security appliances:

- Configuration service
- Authentication service
- Quarantine service
- Log service
- Update service
- Filtering service
- Mail Transfer Agent

The appliance also provides access to the Personal Email Manager and Secure Message Delivery end-user portals.

Software that runs off-appliance

Microsoft SQL Server must be installed off-chassis and must be running before you install the Forcepoint Security Manager.

Download the Forcepoint Security Installer from the Forcepoint Downloads page to install the following off-chassis components:

- Email Security module of Security Manager
- Email Log Server (Windows-only component)
- The Data Security module (Forcepoint DLP) of Security Manager (Windows-only component)

  The Data Security module is required for data loss protection features.

See the Forcepoint Technical Library for more information about components and installation details.

Deployment activity summary

Deploying Forcepoint appliances includes 5 key tasks:

Task 1: Prepare for deployment

Task 2: Setup appliance hardware and create virtual appliances

Task 3: Run the **firstboot** wizard

Task 4: Configure appliances (post-firstboot)

Task 5: Install and configure off-appliance components

Additional configuration steps may be necessary for your deployment. Talk to your Forcepoint distributor and Forcepoint Sales Engineer. Also visit the Forcepoint Deployment and Installation Center.

Forcepoint appliance installation summary

Follow your deployment plan and follow these guides:

- For Forcepoint Email Security, follow the instructions in Installing email protection solutions.
- For Forcepoint Web Security, see Installation Instructions: Forcepoint Web Security.
- For Forcepoint URL Filtering, see Installation Instructions: Forcepoint URL Filtering.

Summary:

1. Microsoft SQL Server must be installed and running to support Forcepoint reporting. Note the location and authentication information for SQL Server.
2. Download the Forcepoint Security Installer from the Forcepoint Downloads page.
3. Rack and cable appliances, and create virtual appliances.
4. Web protection deployments:
   - If your policy source is located off-appliance, install Forcepoint components on that server and start all services before running the firstboot wizard on any appliance. This is because firstboot requires the IP address of the policy source machine and must be able to connect to it. The policy source machine must installed, running, and reachable by appliances before running firstboot.
   - If your policy source is located on an appliance (with X Series, use the blade in Slot-1), ensure that SQL Server is running and reachable from the policy source appliance.
5. Collect data needed by the firstboot wizard. See *The firstboot wizard (initial command-line configuration)*, page 41.

6. Assign each Forcepoint appliance an appropriate domain based on estimated traffic volume.
7. Run the firstboot wizard on every appliance in the deployment. If you're deploying a web protection solution and policy source is located on an appliance, run firstboot on the policy source appliance first.
8. After firstboot has been run on all appliances, use the Forcepoint Security Installer to install additional off-appliance components.
9. Perform post-installation configuration.
10. Install remaining off-appliance components.
11. Configure policies.
12. Test the system.

3 V Series Hardware Setup

Getting Started Guide | V Series Hardware Setup | Version 8.4.x

Related topics:

- *V10000 hardware setup*, page 24
- *V5000 hardware setup*, page 25
- *Using the iDRAC*, page 26
- *Connecting directly to the appliance*, page 27

Deploying Forcepoint appliances includes 5 core tasks. This topic covers **Task 2a**.

Task 1: Prepare for deployment

Task 2: Set up appliance hardware and virtual appliances

a. V Series Hardware Setup (this section)

b. *X Series Hardware Setup*, page 29

c. *Forcepoint Virtual Appliance Setup*, page 39

Task 3: Run the **firstboot** wizard (initial command-line configuration)

Task 4: Configure appliances (post-firstboot)

Task 5: Install off-appliance and optional components

Important

The Quick Start poster packaged in the appliance shipping box shows you all items included in each appliance shipment. This 2-page poster explains how to set up the hardware and shows how to connect cables to the appliance and to your network. You can find appliance Quick Start posters on support.forcepoint.com/documentation.

For instructions on setting up the integrated Dell Remote Access Controller (iDRAC), see *Using the iDRAC*, page 26.

V10000 hardware setup

Forcepoint appliance network interfaces must be able to access a DNS server and the Internet, as described below. This information varies slightly depending on the security mode selected for the appliance.

- *V10000 with Forcepoint Web Security*
- *V10000 with Forcepoint Email Security*

V10000 with Forcepoint Web Security

Network interface C must be able to access a DNS server. This interface typically has continuous access to the Internet. Essential databases are downloaded from Forcepoint servers through interface C (or optionally through P1).

- Ensure that interface C is able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Master Database as well as other security updates. This change must be made in the Web Security module of the Forcepoint Security Manager. In that situation, interface C does not require Internet access.)
- Make sure the C interface IP address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C interface can access.
- If Network Agent is used, network interface N must be connected to a mirror port on a router or switch.

V10000 with Forcepoint Email Security

Network interface E1 (and E2, if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet once the appliance is operational. Essential databases are downloaded from servers through these interfaces.

- Ensure that E1 (and E2, if used) are able to access the download servers at **download.websense.com**.
- Make sure the E1 IP address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the E1 (and E2) interfaces can access.
- Network interface E1 (and E2, if used) must be able to access the mail server.

V5000 hardware setup

The appliance's network interfaces must be able to access a DNS server and the Internet, as described below. This information varies slightly depending on the security mode you select for the appliance.

- *V5000: Forcepoint Web Security*
- *V5000: Forcepoint Email Security*
- *V5000: Forcepoint URL Filtering (no Content Gateway)*

V5000: Forcepoint Web Security

Network interface C must be able to access a DNS server. This interface typically has continuous access to the Internet. Essential databases are downloaded from servers through interface C.

- Ensure that interface C is able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Master Database as well as other security updates. This change must be made in the Web Security module of the Forcepoint Security Manager. In this case, interface C does not require Internet access.)
- Make sure the above addresses are permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C interface can access.
- If Network Agent is used, network interface N must be connected to a mirror port on a router or switch.

V5000: Forcepoint Email Security

Interface P1 (and P2, if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet once the appliance is operational. Essential databases are downloaded from Forcepoint servers through these interfaces.

- Ensure that P1 (and P2, if used) is able to access the download servers at **download.websense.com**.
- Make sure the above addresses are permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the P1 and P2 interfaces can access.
- Network interfaces P1 and P2 (if used) must be able to access the mail server.

V5000: Forcepoint URL Filtering (no Content Gateway)

Network interface C must be able to access a DNS server. Interface C must have continuous access to the Internet. Essential databases are downloaded from Forcepoint servers through this interface.

- Ensure that interface C is able to access the download servers at **download.websense.com**.
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C interface can access.

- If Network Agent is used, network interface N must be connected to a mirror port on a router or switch. Also, if interface N is used to send blocking information, then it must be connected to a *bi-directional* mirror port. Through the bi-directional mirror port, interface N not only monitors all client traffic but also sends blocking information if needed.

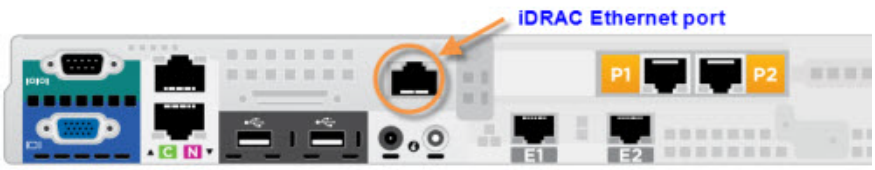
Using the iDRAC

All V Series (and X Series) appliances come with an integrated Dell Remote Access Controller (iDRAC). The iDRAC has its own processor, memory, and network connection. It's many features include power management, virtual media access, and remote console capabilities. It's easily accessed through a web browser or command-line interface.

To set up the iDRAC on a V Series appliance:

1. Cable the iDRAC interface.

   V10000 G4

   V5000 G4

2. In a web browser, go to the iDRAC default IP address

   `https://192.168.0.120`

3. Log on with the default credentials (root/Forcepoint#1, or root/calvin).
4. Go to **Overview > iDRAC Settings > Network** and configure a permanent IP address.

   Applying the new settings causes the iDRAC to close the connection to the browser.
5. Make any needed routing or firewall adjustments to allow a browser to connect to the new IP address on port 443.
6. Open a browser and connect, again, to the iDRAC and log on with the default credentials.
7. Change the default logon password to meet your organization's security requirements. Do not continue to use the factory default password.
   a. Go to **Overview > iDRAC Settings > User Authentication** and click on the number that corresponds to the default log on (root).
   b. Select **Configure User** and click **Next**.

c. Change the password and click **Apply**.

8. To launch the Virtual Console, go to **Overview > Server** and in the upper right Virtual Console Preview area click **Launch**.

To setup the X Series blade server iDRACs, see *Assigning blade slot iDRAC addresses*, page 37.

Connecting directly to the appliance

After hardware setup, it is recommended that you access the appliance console through the iDRAC.

Alternatively, you can:

- Connect a monitor and keyboard directly to the appliance.
- Connect via the serial port. The connection should be set to:
  - 9600 baud rate
  - 8 data bits
  - no parity

4 X Series Hardware Setup

Deploying Forcepoint appliances includes 5 key tasks. This topic covers **Task 2b**.

Task 1: Prepare for deployment

Task 2: Set up appliance hardware and virtual appliances

a. *V Series Hardware Setup*, page 23

b. X Series Hardware Setup (this section)

c. *Forcepoint Virtual Appliance Setup*, page 39

Task 3: Run the **firstboot** wizard (initial command-line configuration)

Task 4: Configure appliances (post-firstboot)

Task 5: Install off-appliance and optional components

Important

The Quick Start poster packaged in the appliance shipping box shows you all items included in each appliance shipment. This 2-page poster explains how to set up the hardware and shows how to connect cables to the appliance and to your network. You can find Appliance Quick Start posters on support.forcepoint.com/documentation.

X10G hardware setup

The X Series X10G appliance includes:

- **X10G blade chassis**: The chassis is an energy-efficient enclosure that holds up to 16 security blades optimized for Forcepoint Web Security and Forcepoint Email Security (installed on separate security blades).
- **X10G security blades**: Security blades are shipped with a hardened operating system and are provisioned with Forcepoint Web Security or Forcepoint Email Security when the **firstboot** wizard is run.

Below is a back view (left) and front view of the chassis, with on-chassis switches enlarged (at lower left) and security blades (at lower right).

Receiving and racking the hardware

The chassis and security blade hardware are manufactured by Dell. All blades are accessible through a web-based integrated Dell Remote Access Controller (iDRAC).

Unloading at your shipping dock

The chassis can weigh up to 400 pounds (182 kilograms) with all hardware components loaded. It is shipped with pre-installed cooling fans, 4 power supply units, 2 switches, and 1 Chassis Management Controller (CMC).

Security blades are typically shipped separately. Insert the security blades after racking the chassis.

Important

You need a loading dock to receive the chassis, or a delivery vehicle with a lift gate.

You will need 4 people to lift the chassis into the rack in your computer room.

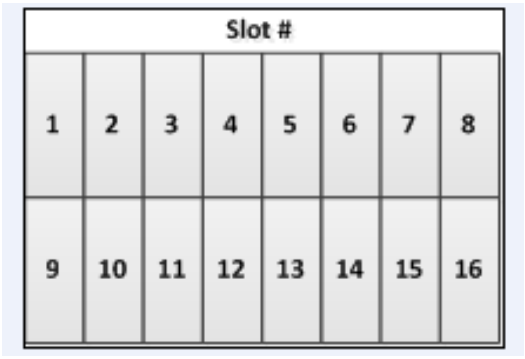
- Unpack and rack the chassis before you insert the security blades. Save the handled cardboard lifter, if a future chassis move is likely.
- Security blades are packaged separately. Blades are imaged with the Forcepoint software you ordered.
- Some Forcepoint components are Windows-only and must be installed and run off the chassis. The installer for these components is named **Forcepoint84xSetup.exe**. Download the installer from the Forcepoint Downloads page.

X10G Quick Start poster

The Quick Start poster packaged in the appliance shipping box shows you all items included in each appliance shipment. This 2-page poster explains how to set up the hardware and shows how to connect cables to the X10G switches and to your network. You can find Appliance Quick Start posters on support.forcepoint.com/documentation.

Security blade slots

Blade slots across the top half of the chassis front are numbered from 1 to 8, beginning at the left as viewed from the front. Bottom slot numbers begin with slot 9 at the left, ending at slot 16.



- **Slot 1**: After racking the chassis, insert the first blade into slot 1. Ensure that any blade inserted into an upper slot is engaged on the hanging rail just inside the top of the slot. When properly engaged, the blade slides easily into the slot. Do not force a blade into a slot. The metal flap covering the backplane in each slot retracts automatically when the blade is inserted.
- **Slots 2 through 16:** Insert blades into consecutive slots, with no empty slots between blades.

iDRAC and interface IP address planning

The Chassis Management Controller (CMC) must be assigned an IP address so that you can communicate with the chassis. This gives you web-based access to the CMC, as shown in this section.

You may need to reserve as many as 67 IP addresses for communication with a single X10G chassis and all of its blade servers.

Many sites use a pattern similar to this: **xxx.xxx.xxx.100** for the IP address of the CMC; **xxx.xxx.xxx.101** for the Integrated DELL Remote Access console (iDRAC) for the blade in slot 1; **xxx.xxx.xxx.102** for the iDRAC of the blade in slot 2; and so on. After the CMC has an IP address assigned, you use a web interface to assign iDRAC IP addresses to all 16 slots as a range. All slots (even empty ones) will have an iDRAC address.

Chassis location	IP address example
CMC	xxx.xxx.xxx.100
Slot 1 Integrated Dell Remote Access Console (iDRAC)	xxx.xxx.xxx.101
Slot 2 iDRAC	xxx.xxx.xxx.102.
Slot 3 iDRAC	xxx.xxx.xxx.103
Slot 4 iDRAC	xxx.xxx.xxx.104
Slot 5 iDRAC	xxx.xxx.xxx.105
Slots 6 through 15	consecutive IP addresses
Slot 16 iDRAC	xxx.xxx.xxx.116

Plan to have a sequential range of IP addresses reserved for the interfaces you plan to use on every blade server (such as C (eth0), P1 (eth1), and optionally P2 (eth2)).

Here is an example for a fully provisioned X10G:

- IP address of CMC might be: `10.8.0.100`
- IP address range (remote access) for 16 blade iDRACs: `10.8.0.101 - 10.8.0.116`
- Subnet mask: `255.255.0.0`
- Gateway IP address: `10.8.0.1`
- The C (eth0) interfaces on the 16 blades might use this IP address range: `10.8.10.201` through `10.8.10.216`
- The P1 (eth0) interfaces on the 16 blades might use this IP address range: `10.9.10.201` through `10.9.10.216`
- The optional P2 (eth1) interfaces on the 16 blades might use IP address range: `10.14.0.101` through `10.14.0.116`
- The IP address of on-chassis switch A1 might be: `10.15.0.121`
- The IP address of on-chassis switch A2 might be: `10.15.0.122`

X10G chassis cabling

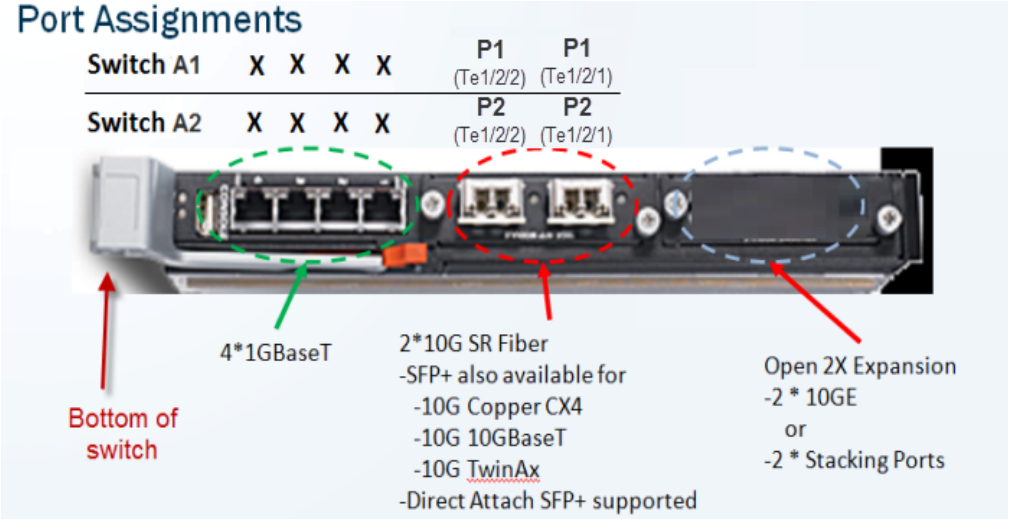
How you cable the X10G depends on your planned deployment. Cabling and deployment options are discussed in detail in the X Series Switch Configuration guide. X10G switches can be configured to support VLAN and switch high availability. By default, the switches are not VLAN-aware.

Before finalizing your cable connections, consult with your Forcepoint partner to ensure that your deployment plans are appropriate for your network traffic. See *Deployment big picture* for related deployment topics and links to other deployment materials.

Power cables, Ethernet cables, a serial cable, and SFP+ cables are shipped with the X10G chassis.

1. Note that the 2 on-chassis switches are oriented vertically at the back of the chassis. The switch on the left side is switch A1. The bottom of the switch is

shown at the left in the diagram below. Use an SFP+ cable or install an optical transceiver and use your own fiber optic cable if desired (see details below).



- Fiber optics: If you ordered an optical transceiver kit with your chassis, see the instructions provided here. This allows you to use fiber optic cables to connect the chassis switches to your network. Begin by connecting the P1 interface on switch A1 to your network. The X10G switch requires an **LC** connector at the end of the optical cable.
- If you are not using fiber optic cables, no transceiver kit is required. Connect an SFP+ cable (provided) to the P1 interface on switch A1.
- While several ports may be labeled on both switches, the only port required for deployment is the P1 port on switch A1. The P2 port on switch A2 is optional and dependent upon your network topology. To ensure correct cabling for your deployment, see the X Series Switch Configuration guide.

2. Next, cable the Chassis Management Controller (CMC). Connect a Category 5 network cable (do not use a crossover cable) from the left-most CMC network port, labeled **Gb** in the illustration, to a switch on the subdomain where the CMC IP address is located.

The CMC is located at the back of the chassis at the upper left side. Connect the **Gb** port to the network.

- Use the power cables to connect the 4 on-board power supply units (PSUs) at the bottom (back of chassis) to the power outlets on your computer rack. Ensure that the power cables are fully inserted into the PSUs and the power source. Confirm that the power lights are illuminated on the PSUs.

Power on

Power on the chassis at the front (recessed button at the lower left corner below slots 9 and 10). This powers on all blades. Blades can also be turned off and on individually.

Set up the CMC IP Address

The X10G chassis includes a small, built-in LCD screen at the lower left front.

With the chassis powered on, pull out the LCD screen and use it to:

1. Set your language preference
2. Specify the IP address of the Chassis Management Controller (CMC)

Setting the CMC IP address enables you to communicate with the controller through a browser, from which you can quickly set remote access (iDRAC) addresses for the blades. The following illustration shows the built-in LCD screen and its associated keypad.

Use the silver arrow pad to the right of the LCD screen to move to a selection. Press the center of the silver pad when you are ready to confirm your choice.

After you choose a language, you are ready to configure the CMC.

LCD Prompt	Recommended response
Configure CMC?	YES
Set Network Speed	Auto (1Gb)
Specify Protocol Type	IP4 Only
IP Addressing Mode	Static

LCD Prompt	Recommended response
Enter static IP address of CMC	xxx.xxx.xxx.xxx
Enter subnet mask for this IP address	xxx.xxx.xxx.xxx
Enter default gateway address for this IP address	xxx.xxx.xxx.xxx
Confirm your settings	(Confirm)
Register DNS?	NO (choose X)
Configure iDRACs?	NO (choose X) You will set these from the web interface.
Apply All Enclosure Settings?	YES

Assigning blade slot iDRAC addresses

Move to a laptop and open a browser that has connectivity to the network where the CMC IP address resides.

Point the browser to the IP address you assigned to the CMC:

```
https://CMC_IP_Address
```

Log on to the CMC with the default credentials (root/Forcepoint#1, or root/calvin).

This enables you to quickly assign consecutive IP addresses for the iDRACs for all 16 blade servers. You will also change the CMC password.

1. Select **Server Overview** at the left and choose the **Setup** tab.
2. Ensure that the **QuickDeploy** check box is enabled.
3. Set **Starting iDRAC IPv4 Address (Slot 1)** from your chosen IP address range for slot iDRACs. (Check the Netmask and Gateway shown on screen, and change if needed.)
4. Click **Save QuickDeploy Settings**.
5. Scroll down, to locate the button labeled **Auto-Populate Using QuickDeploy Settings**. Click it. Contiguous IP addresses are assigned consecutively to all 16 individual slots for iDRACs.
6. **Click Apply iDRAC Network Settings** at the bottom of the screen
7. In the left navigation, select **Chassis Overview > User Authentication**.
8. Select **User ID 1**.

9. Change the password for the CMC and click **Apply**.

X Series hardware setup is complete. Return to your deployment plan for the next step. For example, if you are deploying Forcepoint Web Security, your next step may be to install an off-appliance policy source machine, or if the policy source is on a chassis blade the next step may be to run firstboot on the policy source security blade.

iDRAC Virtual Console

When you are ready to run the **firstboot** wizard on each blade server, sequentially access the iDRAC on each blade and open the Virtual Console to interact with the firstboot wizard. Firstboot runs when you power on the appliance.

To access the iDRAC:

1. Open a Web browser and in the URL entry field enter:

   `https://<blade iDRAC IP address>`
2. Log on with the default credentials (root/Forcepoint#1, or root/calvin)
3. Change the default logon password to meet your organization's security requirements. Do not continue to use the factory default password.
   a. Go to **Overview > iDRAC Settings > User Authentication** and click on the number that corresponds to the default log on (root).
   b. Select **Configure User** and click **Next**.
   c. Change the password and click **Apply**.
4. To launch the Virtual Console, go to **Overview > Server** and in the upper right Virtual Console Preview area click **Launch**.

See *The firstboot wizard (initial command-line configuration)*.

After firstboot completes, remain in the console and log on to the command-line interface (CLI) as 'admin'. Use the password you set during firstboot.

5 Forcepoint Virtual Appliance Setup

A Forcepoint ESXi-hosted VMware virtual appliance can host:

- Forcepoint Email Security
- Forcepoint Web Security

Deploying Forcepoint appliances includes 5 key tasks. This topic covers **Task 2c**.

Task 1: Prepare for deployment

Task 2: Setup appliance hardware and virtual appliances

a. *V Series Hardware Setup*, page 23

b. *X Series Hardware Setup*, page 29

c. Forcepoint Virtual Appliance Setup (this section)

Task 3: Run the **firstboot** wizard (initial command-line configuration)

Task 4: Configure appliances (post-firstboot)

Task 5: Install off-appliance and optional components

Creating a Forcepoint ESXi VMware virtual appliance

VMware virtual appliances are certified with ESXi version 6.0 and supported with v5.5 and other versions of 6.x.

Virtual appliance creation summary

1. Download the OVA from the Forcepoint Downloads page.
2. Use vSphere Client to access the ESXi server.
3. In vSphere Client, run the **Deploy OVF Template** wizard.
   During the procedure you will navigate to and select the downloaded OVA.
4. Power on the VM, open the console, and follow the prompts.

Creating the virtual machine

1. Download the OVA from the Forcepoint Downloads page.
   a. Log on to **MyAccount** (the link above prompts for log on).
   b. Click **Downloads** and on the My Downloads page, click **All Downloads**.
   c. In the Forcepoint Appliance section, locate **Forcepoint Virtual Appliance** and click on **8.4.0**.
   d. Click the entry for the appropriate VMware virtual appliance and download the OVA.
2. Launch vSphere Client and log on to the ESXi server.
3. Run the **Deploy OVF Template** wizard.
   a. On the toolbar, select **File > Deploy OVF Template**.
   b. **Source**: Click **Browse** and then navigate to and select the downloaded OVA file. Click **Next**.
   c. **OVF Template Details**: The OVA file details display. The **Product** is: **Forcepoint_Virtual_Appliance**. Click **Next**.
   d. **Name and Location**: Specify a name, select a location, and click **Next**.
   e. **Host / Cluster**: Select a cluster and click **Next**.
   f. **Resource Pool**: Select a resource pool and click **Next**.
   g. **Storage**: Select a storage location and click **Next**.
   h. **Disk Format**: Select the type of disk provisioning and click **Next**.
   i. **Network Mapping**: Select **VM Network** and click **Next**.
   j. **Ready to Complete**: A deployment settings summary displays. Review and adjust the settings, if needed, and then click **Finish**.

      A progress window reports status of OVA deployment.
4. When OVA deployment is complete, power on the VM and open the console.
5. The appliance configuration process begins with the prompt:

   ```
   Would you like to install the Forcepoint image on this
   machine now? [yes/no]
   ```

   Enter **yes**.
6. When prompted to accept the subscription agreement press **Enter**.

You are now ready to start firstboot.

6 Firstboot Wizard

Getting Started Guide | Firstboot Wizard | Version 8.4.x

Deploying Forcepoint appliances includes 5 key tasks. This topic covers **Task 3**.

Task 1: Prepare for deployment

Task 2: Setup appliance hardware and virtual appliances

Task 3: Run the firstboot wizard (initial command-line configuration)

- *Gather data for firstboot*
- *Run firstboot*

Task 4: Configure appliances (post-firstboot)

Task 5: Install off-appliance and optional components

The firstboot wizard (initial command-line configuration)

The first time you power on (boot) a Forcepoint appliance, a **firstboot** wizard prompts you to:

- Select the security mode for the appliance – Forcepoint Email Security, Forcepoint Web Security, or Forcepoint URL Filtering.
- Enter settings for the appliance management Ethernet interface (C) IP address, subnet mask, default gateway IP address, and DNS server IP addresses.
- Define several basic configuration settings, such as hostname, admin password, and system time zone and time.

You are also asked whether you want to send feedback to Forcepoint. Feedback data improves URL categorization, making your Forcepoint solutions more effective. The default setting is “yes” (enabled). To disable feedback, enter “no” at the prompt. When you upgrade to a major new version, you may be prompted to confirm the setting.

You are given the opportunity to review and change settings before you exit the firstboot wizard. After you approve the settings, the appliance is provisioned and configured. The process can take 30 minutes or more.

Later, if you want to change settings, **except the security mode**, you can make changes using the command-line interface (CLI). To change the security mode, you

must re-image the appliance with an image acquired from the Forcepoint Downloads page. After re-imaging, upon reboot, the firstboot wizard runs again.

Gather data for firstboot

Gather the following information before running the firstboot wizard. Some of this information may have been written down on the Quick Start poster during hardware setup.

Security mode	Chose the security mode that you want to install on the appliance: Forcepoint Email Security, Forcepoint Web Security, or Forcepoint URL Filtering. The security mode must correspond to the product to which you subscribed.
Hostname (example: appliance.example.com) 1 - 60 characters long. The first character must be a letter. Allowed: letters, numbers, dashes, or periods. The name cannot end with a period. If this is a Forcepoint Web Security appliance and Content Gateway will be configured to perform Integrated Windows Authentication, the hostname cannot exceed 11 characters, excluding the domain name. For more information, see the section titled **Integrated Windows Authentication** in Content Gateway Manager Help.	
IP address for appliance management Ethernet interface C	Must be an IPv4 address. Choose an IP address that is not likely to change. Changing the C interface IP address can significantly impact the deployment. For more information, see the technical article Changing the C Interface IP Address.
Subnet mask for network interface C	

Default gateway for network interface C (IP address) *Optional* NOTE: If you do not provide access to the Internet for interface C, use the Web Security module of the Forcepoint Security Manager to configure P1 to download the Master URL Database from Forcepoint servers. Email mode: Configure E1 or P1* to download antispam and antivirus database updates. Configuring these interfaces to access the Internet for database downloads is done through the CLI and through the Security Manager. See the CLI guide for information about configuring the interfaces. See the Administrator Help for the Web Security module and the Administrator Help for the Email Security module for information about configuring database downloads. *On a V5000, use P1; there is no E1 interface.	
Primary DNS server for network interface C (IP address)	
Secondary DNS server for network interface C (IP address) *Optional*	
Tertiary DNS server for network interface C (IP address) *Optional*	
Unified password With Forcepoint Email Security and Forcepoint URL Filtering, the password applies to the CLI. With Forcepoint Web Security the password applies to the CLI and Content Gateway manager. Password length: 8 to 15 characters Include at least one of each of the following: ● Uppercase character ● Lowercase character ● Number ● Special character, such as ! # % & + / [ ] < = > Exclude all of the following: ● The user name of any appliance service account (e.g., admin, root, tech-support, audit) ● Common appliance-related terms (e.g., appliance, filtering) ● The name of the appliance and Forcepoint services (e.g., PolicyBroker or NetworkAgent) ● The device's hostname ● The special characters: space $: ` \ " Do not repeat the previous 3 passwords	

For sites using Forcepoint URL Filtering, the integration method. Choose one: ● Standalone (Network Agent only) ● Microsoft TMG ● Cisco ASA ● Citrix	Choose your third-party integration product, if any.
Send usage statistics?	Usage statistics from appliance modules can optionally be sent to Forcepoint to help improve the accuracy of URL categorization.
For sites using Forcepoint Web Security or Forcepoint URL Filtering, the policy mode of the appliance. ● Full policy mode ● User directory and filtering ● Filtering only NOTE: With Web security mode, the Filtering only policy mode is supported on physical appliances only, not virtual appliances.	**IMPORTANT:** There is only one full policy source machine per deployment. Most sites locate the full policy source installation on a Windows server (off-appliance). An alternative is to configure a V Series or X Series appliance (typically located in Slot-1). The policy mode of remaining appliances is chosen during each appliance's firstboot.

Run firstboot

1. Access the appliance console.
   - With **V Series** or **X Series** appliances, use one of these options.
     - iDRAC: Access the appliance iDRAC and open the virtual console. See *Using the iDRAC*, page 26.
     - Attach a USB keyboard and monitor directly to the appliance.
     - Attach a keyboard and monitor through the serial port.

     Note

     For serial port activation, use:

     - 9600 baud rate
     - 8 data bits
     - no parity

   - With a **VMware virtual appliance**, access the console with the vSphere Client. In vSphere Client, select the virtual machine, open the Console, and click into the window to give it focus.
2. When prompted, read and accept the subscription agreement.
3. At the first prompt, select the security mode. You must have a subscription for the mode you select.

   On an X10G or V10000 appliance, the choices are:

   - Forcepoint Web Security
   - Forcepoint Email Security

On a V5000 appliance, the choices are:

- Forcepoint Web Security
- Forcepoint Email Security
- Forcepoint URL Filtering

On a VMWare virtual appliance, the choices can include:

- Forcepoint Email Security
- Forcepoint Web Security

4. Set the hostname for the device.
5. At the prompt for setting the system time, you have the option to either configure an NTP server or set the time manually.

> **Note**
> If the appliance management interface (C), configured in firstboot, does not have connectivity to the Internet, set the time manually.

   Because all Forcepoint servers in the deployment must be time-synchronized to within 2 minutes, it is recommended that an NTP service be configured for all Forcepoint servers. If necessary, you can configure NTP in the CLI after firstboot.
6. Set the new password.
7. Allow communication with Forcepoint servers. CIDR prefixes can be used with IP addresses to specify subnet mask, default gateway, and DNS information.
8. Continue to follow the on-screen prompts using the information collected above.

After confirming the settings, the wizard applies the configuration and installs the Forcepoint security modules.

X Series Appliances: configure the VLAN settings and confirm settings again.

> **Note**
> Occasionally, due to an I/O timer in the virtual console software, during the software provisioning process firstboot output to the console may stop. To restart console output, simply press Enter.

> **Note**
> If the off-box appliance is unreachable, the system will boot in Full policy mode.

After the wizard completes, stay in the console and log on to the CLI using the password you set during firstboot.

You are now ready for Task 4: *Configure Appliances (post-firstboot)*

7 Configure Appliances (post-firstboot)

Setting up a Forcepoint appliance involves 5 key tasks. This topic covers **Task 4**.

Task 1: Prepare for deployment

Task 2: Setup appliance hardware and virtual appliances

Task 3: Run the firstboot wizard (initial command-line configuration)

Task 4: Configure appliances (post-firstboot)

Task 5: Install off-appliance and optional components

After completing firstboot, finish initial appliance configuration using the command-line interface (CLI). In the CLI you can view system status, configure network and communication settings, and perform general appliance administration tasks. For a complete guide to using the CLI, see the Forcepoint Appliances CLI guide.

Post-firstboot appliance configuration activities include:

- *SSH access to the CLI* (optional)
- *Verify firstboot configuration settings*
- *Establish a filestore*
- *Set an email address for password recovery*
- *Configure additional network interfaces*
- *Configure routes* (if needed)
- *SNMP polling and alerting* (optional)

SSH access to the CLI

After firstboot you may have stayed connected to the appliance console and logged on to the CLI. The method you used to connect to the appliance console remains available to you.

You can also connect to the CLI using a terminal emulator and SSH. SSH access is enabled by default. (Instructions for disabling SSH are included below.)

To connect to the appliance console with SSH, on a Windows system use **PuTTY**, or similar, on a Mac system use **Terminal**. Connect to the appliance management interface (C) IP address on port 22. Use the **admin** credentials set during firstboot.

On V Series or X Series appliances, you can also access the CLI using the Virtual Console feature of the DELL Remote Access Controller (iDRAC), or you can attach a keyboard and monitor directly to the appliance. See the Quick Start poster for your appliance model.

On a VMware virtual appliance, you can also access the CLI through the vSphere Client.

To disable or enable SSH access:

1. Log on to the CLI and change to **config** mode by entering 'config' on the command line. When prompted, enter the admin password again.
2. To display SSH enabled/disabled status:

   ```
   show access ssh --status
   ```
3. To disable or enable SSH access:

   ```
   set access ssh --status <on|off>
   ```

Verify firstboot configuration settings

All system verification and configuration tasks are performed in the CLI. For a complete description of every CLI command, see the Forcepoint Appliances CLI Guide.

To perform the activities in this section, log on to the CLI and enter **config** mode.

Configuration basics

Verify the appliance security mode, policy mode (web protection only), version, and hostname.

```
show appliance info
```

Results may be similar to:

```
Uptime                : 0 days, 2 hours, 13 minutes
Hostname              : webapp.example.com
Hardware_platform     : V10000 G4
Appliance_version     : 8.4.0
Mode                  : Forcepoint Web Security
Policy_mode           : Filtering only
Policy_server_ip      : 10.222.10.10
```

Appliance management interface (C)

Display the network interface settings and confirm the settings for interface C.

```
show interface info
```

Note
IPv4 addresses must be used with all Forcepoint management interfaces.

Warning
After configuration in firstboot, do not change the C interface IP address. If you must change the C interface IP address, see the article Changing the C Interface IP Address.

Be cautioned that the **set interface ipv4** command allows you to change the configuration of any available network interface, including interface C.

To change the appliance DNS settings:

```
set interface dns --dns1 <IPv4_address>
   [--dns2 <IPv4_address> --dns3 <IPv4_address>]
```

System time and time synchronization with Forcepoint servers

Display the system time and time zone.

```
show system clock
show system timezone
```

To display the NTP status:

```
show system ntp
```

Within a deployment, the clock on all Forcepoint servers must be synchronized to within 2 minutes.

Important

Before changing the time, stop all Forcepoint services running in your network. Then, reset the time and make certain that the time is consistent across all servers running Forcepoint services. Finally, restart Forcepoint services.

If you do not stop the services first, client updates and policy changes entered after the time reset are not saved.

For reliability and ease of maintenance, configuring an Internet Network Time Protocol (NTP) server (www.ntp.org) is recommended. If the appliance management interface (C) is not connected to the Internet, then you must provide a way for interface C to reach an NTP server. One solution is to install an NTP server on the local network where it can be reached by interface C.

Important

If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between the appliance and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server.

To enable and configure an NTP server:

```
set system ntp --status on
set system ntp --server <server1>,<server2>,<server3>
```

server can be an IP address or URL. The URL is restricted to letters, numbers, hyphens (-), and periods (.). A URL must begin with a letter or number.

To sync with an NTP server:

```
sync system ntp
```

To set the system time manually:

```
set system timezone
set system clock
```

The default time zone is GMT (Greenwich Mean Time), also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.

Time is set using 24-hour notation.

Add an appliance description

Optionally, to help you identify and manage the system, add a unique appliance description. This is particularly helpful when there are multiple Forcepoint appliances in the deployment.

Use the commands:

```
show system host
set system host --description '<description>'
```

description must be enclosed in single or double quotation marks. Length is limited to 100 characters.

Establish a filestore

A **filestore** is an off-appliance (remote) storage location for storing appliance-related files, including backup, log, and configuration files.

Establishing a filestore is essential because any file that you want to save or load, must be done with a filestore. Only system backup and log files are kept on the appliance.

A filestore definition includes:

- A unique name, known as the filestore alias.
- The IP address of the filestore host and the port on which to connect.
- The directory location (path) on the host.
- The protocol to use to connect and move files to and from the filestore. Supported protocols include **ftp**, **tftp**, and **samba**.
- Optionally, the name of a user (account) with permissions on the filestore.

To define a filestore:

```
set filestore --alias <name> --type <ftp|tftp|samba>
   --host <ip_address> --path <share_directory>
   [--user <user_name>] [--port <port>]
```

Example:

```
set filestore --alias fstore --type samba
   --host 10.123.48.70 --path myfiles/myfolder --user jdoe
```

Set an email address for password recovery

Set an email address and SMTP server in the event that the **admin** password is forgotten or lost. A temporary password is sent to the address when an administrator enters Ctrl+P at the CLI logon prompt.

To set an email address and SMTP server:

```
set account email --address <email_address>
set account smtp --host <location> --port <port>
   --user <name>
```

To test the settings use:

```
send test_email
```

When no email address is set, Ctrl+P prompts to confirm that a password reset is wanted. When confirmed (yes), a security code is displayed. Write it down. To get a temporary password, contact Technical Support and provide the security code.

Configure additional network interfaces

Already configured: *Appliance management interface (C)*

In addition to the appliance management interface, set during firstboot, one or more additional network interfaces must be configured. Interfaces can be configured with DHCP.

- *Content Gateway (web proxy) interfaces (P1 and P2)*
- *Web protection: Network Agent interface (N)* (use of Network Agent is optional)
- *Forcepoint Email Security interfaces (E1 and E2, or P1 and P2)*
- *Interface bonding* (optional)

Support for IPv6

- Forcepoint Email Security does not support IPv6.
- IPv6 support in Forcepoint Web Security and Forcepoint URL Filtering is **disabled** by default.

> **Important**
> After IPv6 support is enabled, subsequent disablement requires a full restart of the appliance.

For all web security solutions, IPv6 support includes:

- Dual IP stack configuration for interfaces C and N
- IPv6 traffic to the Internet or clients on interfaces C and N, including block pages sent on C or N
- IPv6 static routes
- SNMP traps and counters for IPv6 data
- Network diagnostic tools in the CLI

For Forcepoint Web Security, IPv6 support also includes:

- Dual IP stack implementation on interfaces P1 and P2
- Traffic to the Internet or clients on interfaces P1 and P2, and their bonded interface (E1/E2), if configured

Limits and restrictions:

- IPv6-only internal networks are not supported
- IPv4 must be used to communicate among appliances and Forcepoint components

In any field that accepts an IPv6 address, the address can be entered in any format that conforms with the standard. For example:

- Leading zeros within a 16-bit value may be omitted.

- One group of consecutive zeros may be replaced with a double colon.

Appliance management interface (C)

The appliance management interface (C) is configured during **firstboot**.

The appliance management interface:

- Communicates with Forcepoint management interfaces
- Provides inter-appliance communication
- Optionally, transports non-HTTP and non-HTTPS protocol enforcement (typically handled on interface N).
- Handles Master Database downloads via the Internet (unless P1 is configured for database downloads).

Important

Changing the C interface IP address can significantly impact the deployment. If at all possible, do not change the C IP address. If you must change the C IP address, see the technical article Changing the C Interface IP Address.

Guidelines for configuring network interface C

IP address (C interface)	Required. Should not be changed after initial configuration in firstboot. This interface typically requires continuous access to the Internet, though some sites use P1 for all communication with the Internet.
Subnet mask (C)	Required.
Default gateway (C)	Required. IP address of the router that allows traffic to be routed outside of the subnet.
Primary DNS (C)	Required. IP address of the domain name system server.
Secondary DNS (C)	Optional. Serves as a backup in case the primary DNS server is unavailable.
Tertiary DNS (C)	Optional. Serves as a backup in case the primary and secondary DNS servers are unavailable.

Content Gateway (web proxy) interfaces (P1 and P2)

Content Gateway interfaces P1 and P2 handle traffic directed to and from the Content Gateway proxy module.

- Both the P1 and P2 proxy interfaces can be used to accept users' Internet requests (inbound traffic) and communicate with web servers (outbound traffic). In other words, both interfaces can be configured to handle traffic into and out of the proxy module.
- A typical configuration is to use P1 for both inbound and outbound traffic; P2 is not used.
- Another option is to configure P1 to accept users' Internet requests (inbound only). In this case, P2 is configured to communicate with web servers (outbound).

Important

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Content Gateway.

For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCP router. In this case, you must configure Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager, see the General tab of the **Configure > Networking > WCCP** page).

To view the interface bindings in the CLI:

```
(view)# show interface info
```

Guidelines for configuring network interfaces P1 and P2

IP address (P1 or P2 interface)	Required.
Subnet mask	Required.
Default gateway	Optional. The gateway must be in the same subnet as the IP address of the interface (P1 or P2) used for communicating with the Internet (outbound traffic). Ensure that outbound packets can reach the Internet.
Primary DNS	Required. IP address of the domain name system.
Secondary DNS	Optional. Serves as a backup in case the primary DNS server is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNS servers are unavailable.

CLI example:

```
(config)# set interface ipv4 --interface p1
          --ip 10.200.200.20 --mask 255.255.0.0
          --gateway 10.200.0.5
(config)# set interface dns --module proxy
          --dns1 10.10.10.10 --dns2 10.10.10.11
```

Web protection: Network Agent interface (N)

Network Agent is an optional component of Forcepoint Web Security and Forcepoint URL Filtering solutions. When used with Forcepoint Web Security, it can provide security for protocols other than HTTP and HTTPS. It also provides bandwidth optimization data and enhanced logging detail.

Network Agent is typically configured to see both inbound and outbound traffic in your network. The agent distinguishes between:

- Requests sent from internal machines to internal machines (hits to an intranet server, for example)
- Requests sent from internal machines to external machines such as web servers (user Internet requests, for example)

You choose whether blocking information for non-HTTP protocols is routed through interface C or interface N.

Note
Network Agent is supported on V Series appliances and on standalone servers.

Guidelines for configuring network interface N

Important
Network interface N configuration is only necessary when Network Agent is installed and running on the appliance and you want blocking to go through interface N.

IP address of interface N	Required. Network Agent should be able to see the outbound and inbound traffic in your network. Network Agent ignores ports 80, 443, 8070, and 8080.
Subnet mask	Required.
Default gateway	Required.
Primary DNS	Required. IP address of the domain name system server.

Secondary DNS	Optional. Serves as a backup in case the primary DNS server is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNS servers are unavailable.

CLI example:

```
(config)# set interface ipv4 --interface n
          --ip 10.200.200.20 --mask 255.255.0.0
          --gateway 10.200.0.5
(config)# set interface dns --module network-agent
          --dns1 10.10.10.10 --dns2 10.10.10.11
```

Network Agent can instead be installed on a different server in the network.

Forcepoint Email Security interfaces (E1 and E2, or P1 and P2)

Forcepoint Email Security interfaces handle traffic into and out of the email module. Set up interfaces E1 (P1), E2 (P2), and C correctly before deploying off-appliance components.

Note

The names of the interfaces vary depending on appliance model.

- On V10000, E1 and E2 are used.
- On V5000, X10G, and virtual appliances, P1 and P2 are used.

- Both the E1 (P1) and E2 (P2) interfaces can be used to accept inbound traffic and send outbound traffic.
- A typical configuration is to use E1 (P1) for both inbound and outbound traffic; E2 (P2) is not used.
- Another option is to configure E1 (P1) to accept inbound and E2 (P2) to send outbound traffic.

- When you need to support a large volume of outbound traffic, you can configure virtual interfaces on E1 or E2 (P1 or P2).

Important

On the V10000, if you use the E2 interface, the E1 interface is bound to eth0, and the E2 interface is bound to eth1. Keep this in mind when you configure Forcepoint Email Security.

On other appliances, if you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Forcepoint Email Security.

Guidelines for configuring network interfaces E1 (P1) and E2 (P2)

IP address (E1 or E2 interface)	Required. E1 (P1) is used by default to connect to SQL Server for reporting. If E1 does not have a valid IP address or does not have DNS access, then Forcepoint Email Security cannot resolve the SQL Server hostname and cannot create a connection with SQL Server. Off-box installation of the management console is then blocked.
Subnet mask	Required.
Default gateway	Required. The gateway must be in the same subnet as the IP address of the interface (E1 or E2) used for communicating with the Internet (outbound traffic). Ensure that outbound packets can reach the Internet.
Primary DNS	Required. IP address of the domain name system server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS server is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNS servers are unavailable.

CLI example:

```
(config)# set interface ipv4 --interface e1
          --ip 10.200.200.20 --mask 255.255.0.0
          --gateway 10.200.0.5
(config)# set interface dns --module email
          --dns1 10.10.10.10 --dns2 10.10.10.11
```

Interface bonding

V10000 appliances can bond interfaces for failover or load balancing. Configuration details are provided below.

Interface bonding is not supported on V5000, X10G, or virtual appliances.

Important
Do not bond interfaces that have different speeds or duplex modes. Doing so can result in performance problems.

V10000 with Forcepoint Web Security

Interfaces E1 and E2 can be cabled to your network and then bonded through software settings to a Content Gateway interface, with E1 optionally bonded to P1, and E2 optionally bonded to P2. No other pairing is possible.

Interface bonding provides these alternatives:

- Active/Standby mode: P1 (or P2) is active, and E1 (or E2) is in standby mode. Only if the primary interface fails would its bonded interface (E1 or E2) become active.
- Load balancing: If the switch or router that is directly connected to the V10000 supports load balancing (etherchannel, trunk group, or similar), then traffic to and from the primary interface can be balanced between the primary interface and its bonded interface (E1 or E2).

You can choose to bond or not bond each Content Gateway interface independently. You do not have to bond at all.

If you do bond an interface, choose one mode for that bonding (either active/standby or load balancing). You do not have to choose the same bonding mode for both interfaces.

Ensure that all interfaces are cabled properly before bonding.

V10000 with Forcepoint Email Security only

Interfaces P1 and P2 can be cabled to your network and then bonded through software settings to a Forcepoint Email Security interface, with P1 optionally bonded to E1, and P2 optionally bonded to E2. No other pairing is possible.

Interface bonding provides these alternatives:

- Active/Standby mode: E1 (or E2) is active, and P1 (or P2) is in standby mode. Only if the primary interface fails would its bonded interface (P1 or P2) become active.
- Load balancing: If the switch or router that is directly connected to the V10000 supports load balancing (etherchannel, trunk group, or similar), then traffic to and from the primary interface can be balanced between the primary interface and its bonded interface (P1 or P2).

You can choose to bond or not bond each Forcepoint Email Security interface independently. You do not have to bond at all.

If you do bond an interface, choose one mode for that bonding (either active/standby or load balancing). You do not have to choose the same bonding mode for both interfaces.

Ensure that all interfaces are cabled properly before bonding.

CLI example:

```
(config)# set interface bond --mode active-standby
```

Configure routes

You can use CLI route commands to specify:

- Static routes from subnets and client computers through any active appliance interface, except N.

  If IPv6 is enabled, static IPv6 routes can also be added and imported.
- Component routes from appliance modules through appliance interface C to subnets.

  IPv6 component routes are not supported.

Static routes

- The same route cannot be added for 2 different interfaces on the same module. If attempted, an error message displays.
- Static routes that are defined for an interface that is later made inactive remain in the routing table.
- Static routes that become invalid because the IP address of the interface changes are disabled.
- Static routes can be added and deleted, but not modified. To modify a route, delete it and add a new route specifying the new values.
- Static routes can be bulk added from a text file. See the Forcepoint Appliances CLI Guide.
- The static route table has a maximum limit of 5000 entries.

CLI example:

```
(config)# set route --dest 11.0.0.0 --mask 255.0.0.0
          --gateway 10.206.7.254 --interface c
(config)# set route6 --dest 2222:3333:4444:5555::0
          --interface p1 --prefixlen 64
          --gateway 1234:5678::8765:4321
```

Component routes

Although the appliance management interface (C) is typically reserved for management traffic, in some deployments it is necessary or desirable to route some web or email traffic through the C interface rather than P1/P2 or E1/E2.

The component route table has a maximum limit of 5000 entries.

CLI example:

```
(config)# set component_route --dest 11.0.0.0
          --mask 255.0.0.0 --module email
```

SNMP polling and alerting

Forcepoint appliances can issue alerts using SNMP trap data when integrated with a supported Security Information Event Management (SIEM) system. SNMP traps send alerts to system administrators about significant events that affect the security of the network.

In the CLI, the appliance can be configured to:

- Allow your SNMP manager to poll the appliance for standard SNMP counters.
- Send SNMP traps for selected events to your SNMP manager.

Support is included for SNMP v1, v2c, and v3.

- With SNMP v1 and v2c, a suffix (-proxy, -web, -na, or -email) is appended to the community name to indicate the originating module for the counter.
- With SNMP v3, you can specify the context name (Proxy, Web, NA, or Email) to poll counters for each module.

If you use v1 or v2c, you must specify the community name for the appliance.

If you use v3, you must specify security level, user, authentication, and encryption type to associate with SNMP communication.

To enable polling:

```
set snmp service --status on
set snmp version --options <values>
```

SNMP traps

SNMP monitor service and SNMP trap settings are independent, but SNMP monitor service must be enabled before you activate the SNMP trap configuration.

Use these commands to work with SNMP traps:

```
show snmp config
show trap config
show trap events
set snmp service
set trap service
set trap version (v1, v2c, v3) --options <values>
save trap --location <filestore_alias>
load trap --location <filestore_alias> --file <name>
save mibfile --location <filestore_alias>
test trap event
```

Use ‘test trap event’ to verify your configuration. If there is a problem sending the test trap, verify the community name, IP address, and port, and make sure that the network allows communication between the appliance and the SNMP manager.

See the Forcepoint Appliances CLI Guide.

8 Installation of Off-Appliance Components

Setting up a Forcepoint appliance involves 5 key tasks. This topic covers **Task 5**.

Task 1: Prepare for deployment

Task 2: Setup appliance hardware and virtual appliances

Task 3: Run the **firstboot** wizard (initial command-line configuration)

Task 4: Configure appliances (post-firstboot)

Task 5: Install off-appliance and optional components

After the appliance has been configured, install the remaining off-appliance components. See your deployment plan. For a refresher, see *Required off-appliance components*, page 14.

To install off-appliance components, return to the following guides.

- Forcepoint Email Security: Installing email protection appliance-based solutions.
- Forcepoint Web Security: Installation Instructions: Forcepoint Web Security.
- Forcepoint URL Filtering: Installation Instructions: Forcepoint URL Filtering.