

Quick Start Guide

Forcepoint V10000 G3

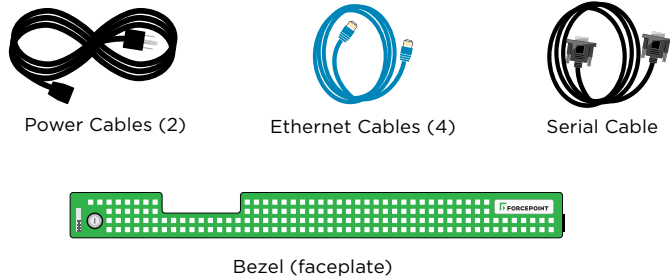
Web or Email Security Appliance

⚠ Before you begin...

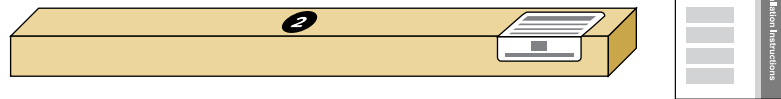
Plan your deployment before setting up the appliance. See the back of this guide for a deployment overview and reference sheet.

1 Verify Contents

1 Accessory Kit

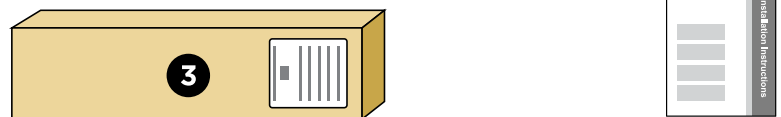


2 Sliding Ready Rail Kit



- Left Ready Rail
- Right Ready Rail
- Velcro Straps (2)
- Rack Installation Instructions

3 Cable Management Arm Kit



- Cable Management Arm
- Cable Tie Wraps
- Static Support Tray
- CMA Installation Instructions

Contact Forcepoint Technical Support if any items are missing.

2 Rack Appliance



See the **Rack Installation Instructions** included in the Sliding Ready Rail kit.

3 Determine Security Mode

The appliance supports the following security modes:

- **Web** (Forcepoint Web Security)
- **Email** (Forcepoint Email Security)

Based on your subscription and deployment plan, determine the appropriate security mode for this appliance.

4 Connect Network Cables

Connect the appliance interfaces required by the security mode for this appliance. *Cat 5E cables (or better) are required. Do not use crossover network cables.*

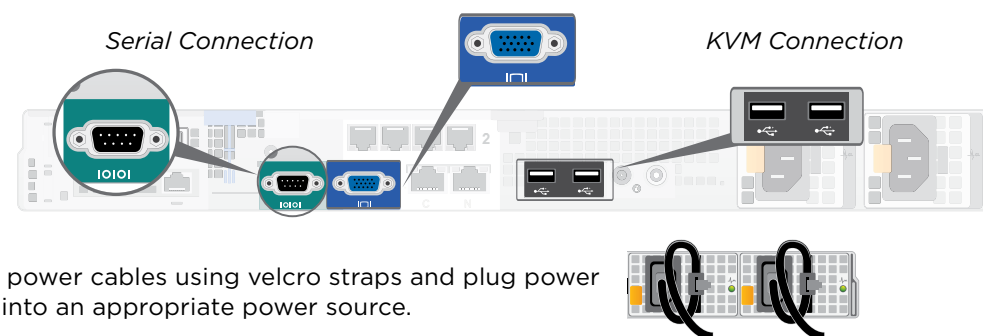
	Web	Email
Required Ports:	C, P1, N	C, E1
Optional Ports:	P2, E1, E2	E2, P1, P2



Interface	Function
C	<ul style="list-style-type: none"> • Provides communication with other Forcepoint components, including Forcepoint Security Manager. • Handles database downloads from the Internet. • Provides access to the Content Gateway Manager.
P1, P2	<ul style="list-style-type: none"> • Enables Content Gateway proxy to receive Internet requests and communicate with Web servers. • Optionally bonded to E1/E2 in Email mode.
N	<ul style="list-style-type: none"> • Allows Network Agent to monitor Internet requests. • Connect to switch port. If sending blocking information through N, connect to bidirectional span, monitor, or mirror port on switch.
E1, E2	<ul style="list-style-type: none"> • Enables Forcepoint Email Security to receive and send mail. • Provides personal email management and cluster communication. • Requires access to mail server. • Optionally bonded to P1/P2 in Web mode.

5 Connect Input Device

1. Connect to the appliance via serial port or KVM in order to access the command line interface for initial configuration. *Serial port settings are: 9600 baud, 8 bits, no parity.*



2. Secure power cables using velcro straps and plug power cables into an appropriate power source.

6 Power On Appliance

Power on the appliance and check the following indicators:

Front

- Power button is illuminated.
- Hard drive LEDs are green.

Rear

- Power supply LEDs are green.
- LEDs for connected interfaces (NICs) are green.
- System status indicator (LED left of power supplies) is solid blue.

Contact Forcepoint Technical Support if any indicators are not illuminated correctly.

7 Configuration Overview

Please refer to the **Forcepoint Appliances Getting Started** guide for more details.

Initial Configuration

Firstboot Script

- Configure security mode.
- Configure the appliance management communication interface (C).
- Configure NTP servers/system time.

Appliance Command Line

- Configure applicable network interfaces.
- Configure other settings as desired.

Web Mode

Forcepoint Security Manager

- Enter subscription key, update Master Database, configure Network Agent, and configure policies in Forcepoint Security Manager.
- Requires Windows Server 2008 R2, or Windows Server 2012 or 2012 R2, or Windows Server 2016.

Content Gateway Manager (proxy)

- Configure user authentication and select protocols.

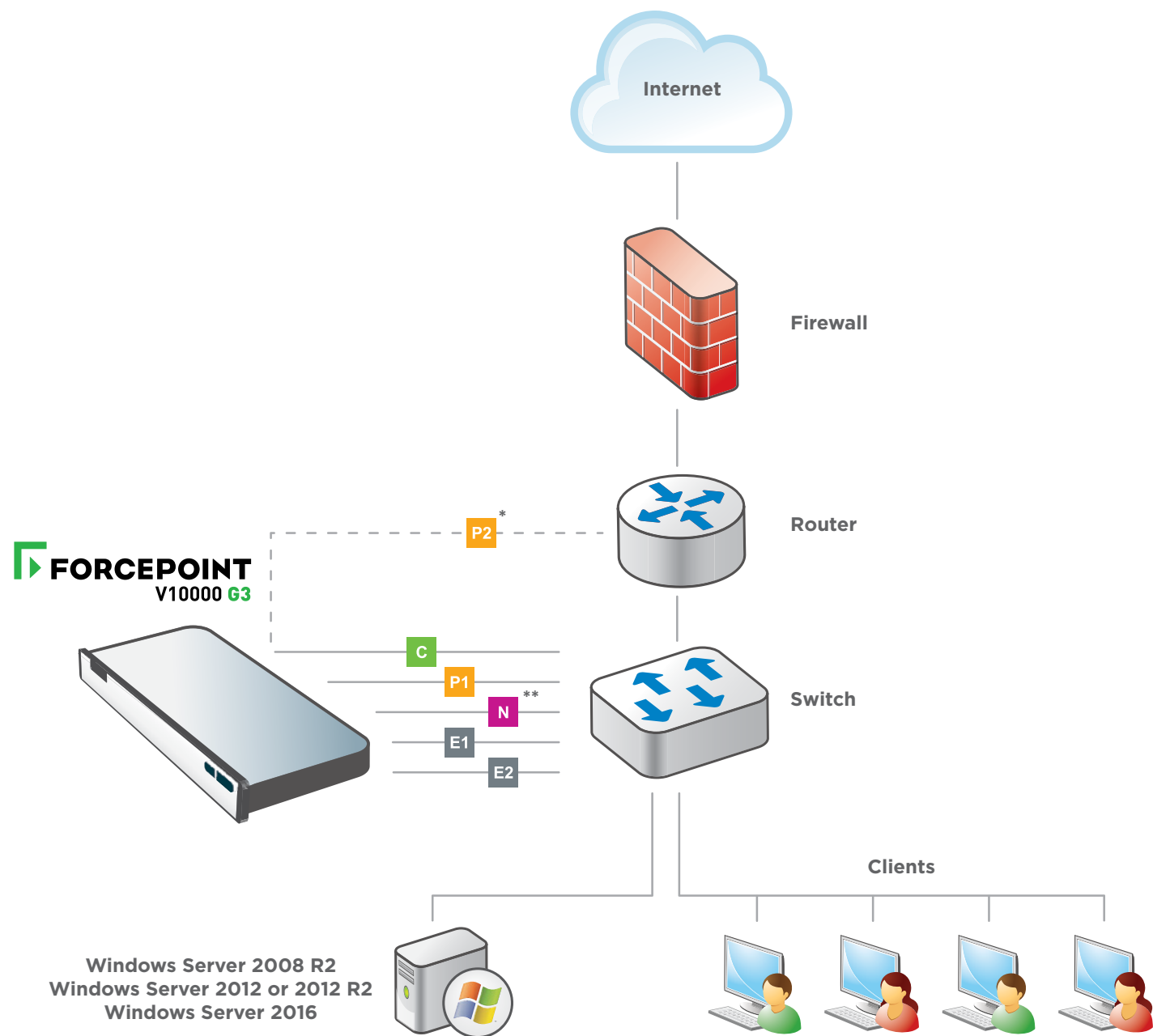
Email Mode

Forcepoint Security Manager

- Complete configuration wizard, enter subscription key, and configure policies in the Email Security module. Configure email DLP policies in the Data Security module.
- Requires Windows Server 2008 R2, or Windows Server 2012 or 2012 R2, or Windows Server 2016.

Appliance Deployment Overview

You can deploy one or more appliances on your network. The diagram below illustrates a basic appliance deployment. A separate computer with Windows Server is required for running Forcepoint Security Manager. See the **Forcepoint Appliances Getting Started** guide for details.



* P2 is optional and may be connected to a router or switch.

** Connect to bidirectional span, monitor, or mirror port if sending blocking information through N.

Support & Resources

Getting Started Guide

support.forcepoint.com/documentation

Online Support and Contact Information

support.forcepoint.com

Deployment Reference Sheet

Appliance Information

Interface C IP:

Hostname:

admin is the default user name for the Appliance CLI, Forcepoint Security Manager, and Content Gateway Manager.

Network Configuration

Appliance Management Communications Interface (C)

IP Address:

Primary DNS:

Subnet Mask:

Secondary DNS:

Default Gateway:

Tertiary DNS:

Content Gateway Interfaces (P1 & P2)

P1

IP Address:

Default Gateway:

Subnet Mask:

Primary DNS:

P2

IP Address:

Secondary DNS:

Subnet Mask:

Tertiary DNS:

Above settings apply to P1 and P2

Network Agent Interface (N)

IP Address:

Primary DNS:

Subnet Mask:

Secondary DNS:

Default Gateway:

Tertiary DNS:

Forcepoint Email Security Interfaces (E1 & E2)

E1

IP Address:

Default Gateway:

Subnet Mask:

Primary DNS:

E2

IP Address:

Secondary DNS:

Subnet Mask:

Tertiary DNS:

Above settings apply to E1 and E2

Forcepoint Security Manager

Web

Policy Server IP:

SQL Server

IP Address:

Log Server IP:

User Name:

Subscription Key:

Password:

Email

Log Server IP:

Authentication Mode:

See the **Forcepoint Appliances Getting Started** guide for details.