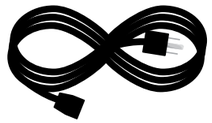
Quick Start Guide
Forcepoint V5000 G4R2
Web or Email Security Appliance

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

Ethernet Cables (4)



Power Cable

Serial Cable

Bezel (faceplate)

Rack tray/rail kit not included. Optional Static Rail Kit available. Contact your Forcepoint account representative.

Contact Forcepoint Technical Support if any items are missing.

2 Rack Installation

To mount the V5000 appliance, use a rack tray or rail kit (not included). If using a rack tray:

1. Install rack tray into desired server rack.

2. Place appliance on tray and secure to server rack using mounting screws on front of appliance.

3 Determine Security Mode

The appliance supports the following security modes:

- **Web** (Forcepoint Web Security or Forcepoint URL Filtering)
- **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	P1
Optional Ports:	P2*	iDRAC		P2	iDRAC

**Not used for Forcepoint URL Filtering.*

Interface	Function
C	• Provides communication with other Forcepoint components, including Forcepoint Security Manager. • Handles database downloads from Internet.
P1 P2	**Web mode:** • Enables Content Gateway proxy to receive Internet requests and communicate with web servers. **Email mode:** • Enables Forcepoint Email Security to receive and send mail. • Provides personal email management and cluster communication. • Requires access to mail server.
N	• 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.
iDRAC	• Preferred method for managing the server. • Allows remote management. • See Knowledge Base article #11964 for more information.

5 Connect Input Device & Power On

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.

Notes:

- Get the default iDRAC password from the Dell information tag.
- Best practice: 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.

Rear

- 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 (see latest Security Manager release notes for supported versions).

Content Gateway Manager (proxy)

- If your site uses the Forcepoint proxy, configure user authentication and select protocols.

Email Mode

Forcepoint Security Manager

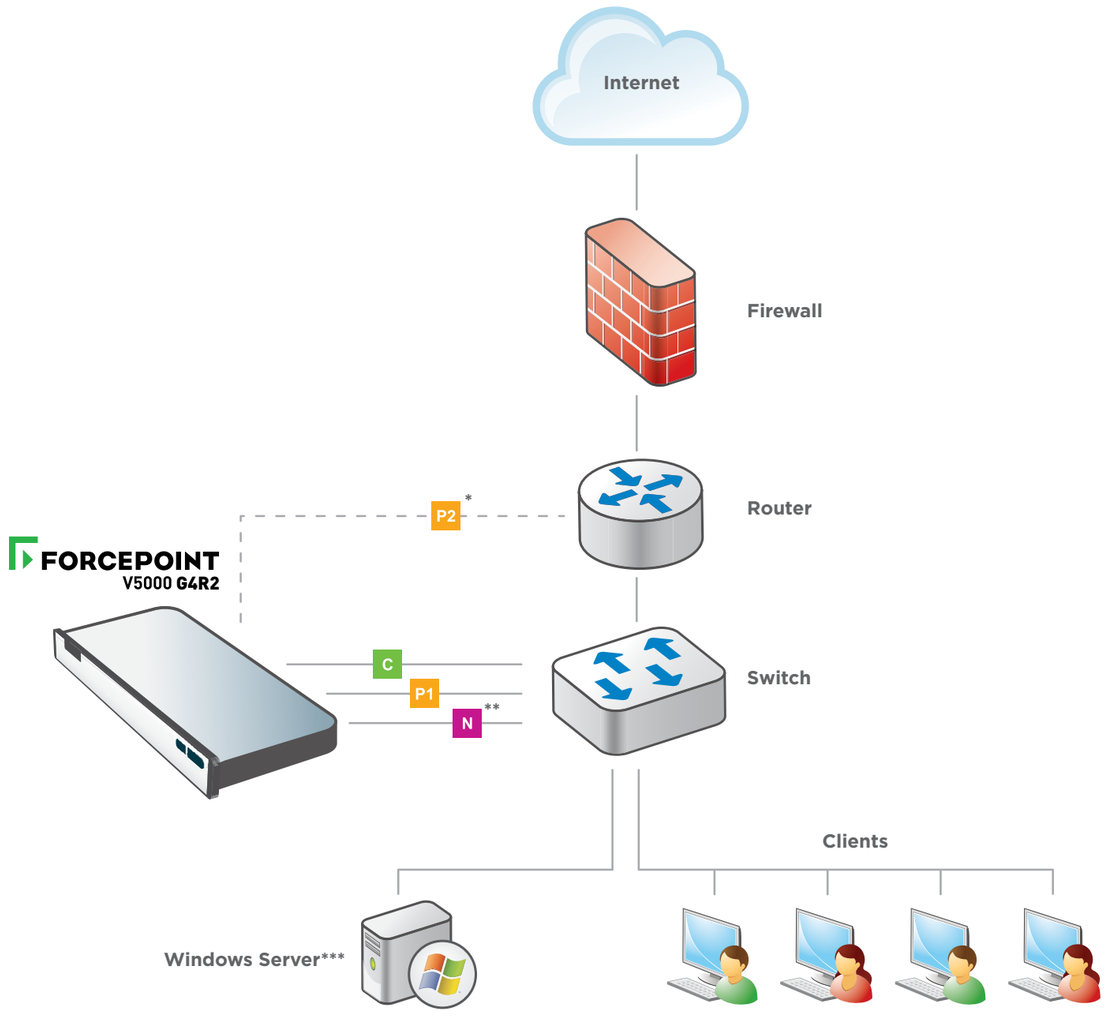
- Complete configuration wizard, enter subscription key, and configure policies in the Email Security module. Configure email DLP policies in the Data Security module.
- Requires Windows Server (see latest Security Manager release notes for supported versions).

FORCEPOINT
V5000 G4R2

QSG240-100_RevA

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 the N interface to a bidirectional span, monitor, or mirror port on the switch.
*** Forcepoint Security Manager is required; Forcepoint Security Appliance Manager (FSAM) is optional.

Support & Resources

Getting Started Guide
support.forcepoint.com/documentation

Online Support and Contact Information
support.forcepoint.com

Deployment Reference Sheet

Appliance Information

C Interface IP: _____ Hostname: _____

Default iDRAC password: _____

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

Network Configuration

Appliance Management Communication Interface (C)

IP Address: _____ Primary DNS: _____

Subnet Mask: _____ Secondary DNS: _____

Default Gateway: _____ Tertiary DNS: _____

Content Gateway / Forcepoint Email Security Interfaces (P1 & P2)

P1

IP Address: _____ Default Gateway: _____

Subnet Mask: _____ Primary DNS: _____

Secondary DNS: _____

P2

IP Address: _____ Tertiary DNS: _____

Subnet Mask: _____

Above settings apply to P1 and P2

Network Agent Interface (N)

IP Address: _____ Primary DNS: _____

Subnet Mask: _____ Secondary DNS: _____

Default Gateway: _____ Tertiary DNS: _____

Forcepoint Security Manager

Web

Policy Server IP: _____

Log Server IP: _____

Subscription Key: _____

SQL Server

IP Address: _____

User Name: _____

Password: _____

Email

Log Server IP: _____

Authentication Mode: _____

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