

# Quick Start Guide

Forcepoint V20000 G5  
Forcepoint V10000 G5



## 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



Power Cables (2)

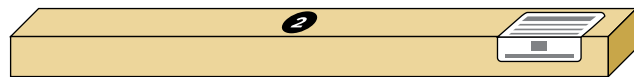


Ethernet Cables:  
6 - For V10000 G5  
None - For V20000 G5



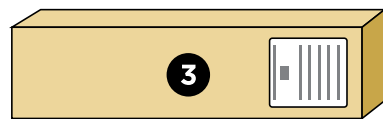
Bezel (faceplate)

### 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.

Optional 10GbE NIC Expansion Kit available for V10000 G5. Contact your Forcepoint account representative.

## 2 Rack Appliance



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

## 3 Determine Security Mode

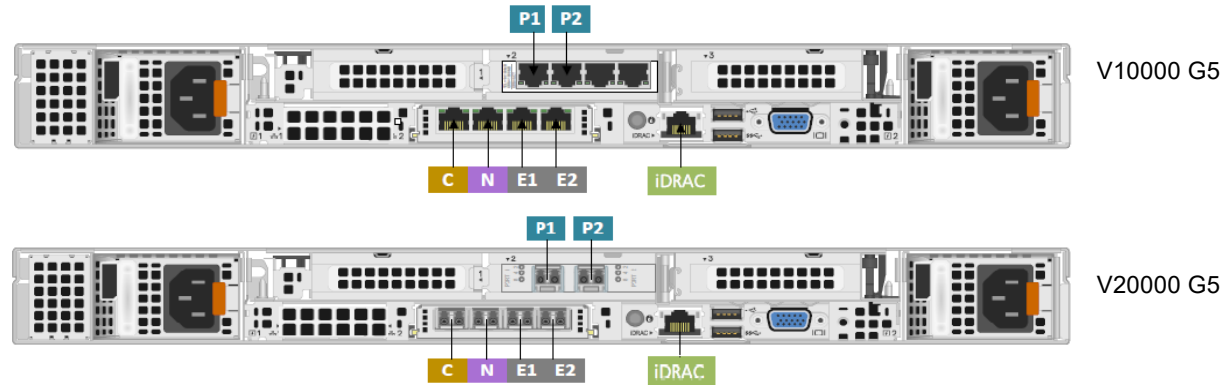
The appliance supports the following security modes:

- **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

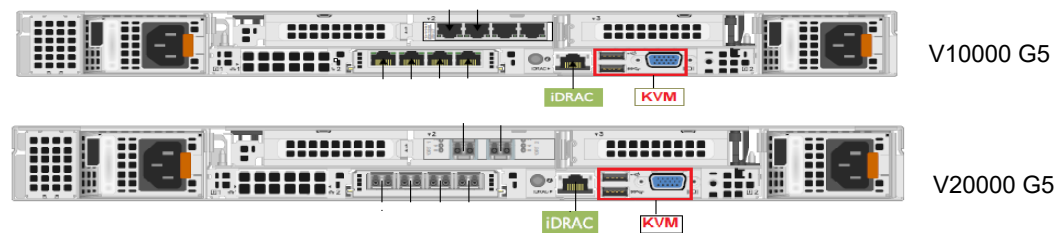
Cat 5E cables (or better) are required. Do not use crossover network cables. If optional 10GbE optical NIC is selected, please refer to 10GbE PCI NIC Installation Guide.



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

## 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 URL Database, configure Network Agent, and configure policies in Forcepoint Security Manager.

#### Content Gateway Manager (proxy)

Configure user authentication and select protocols.

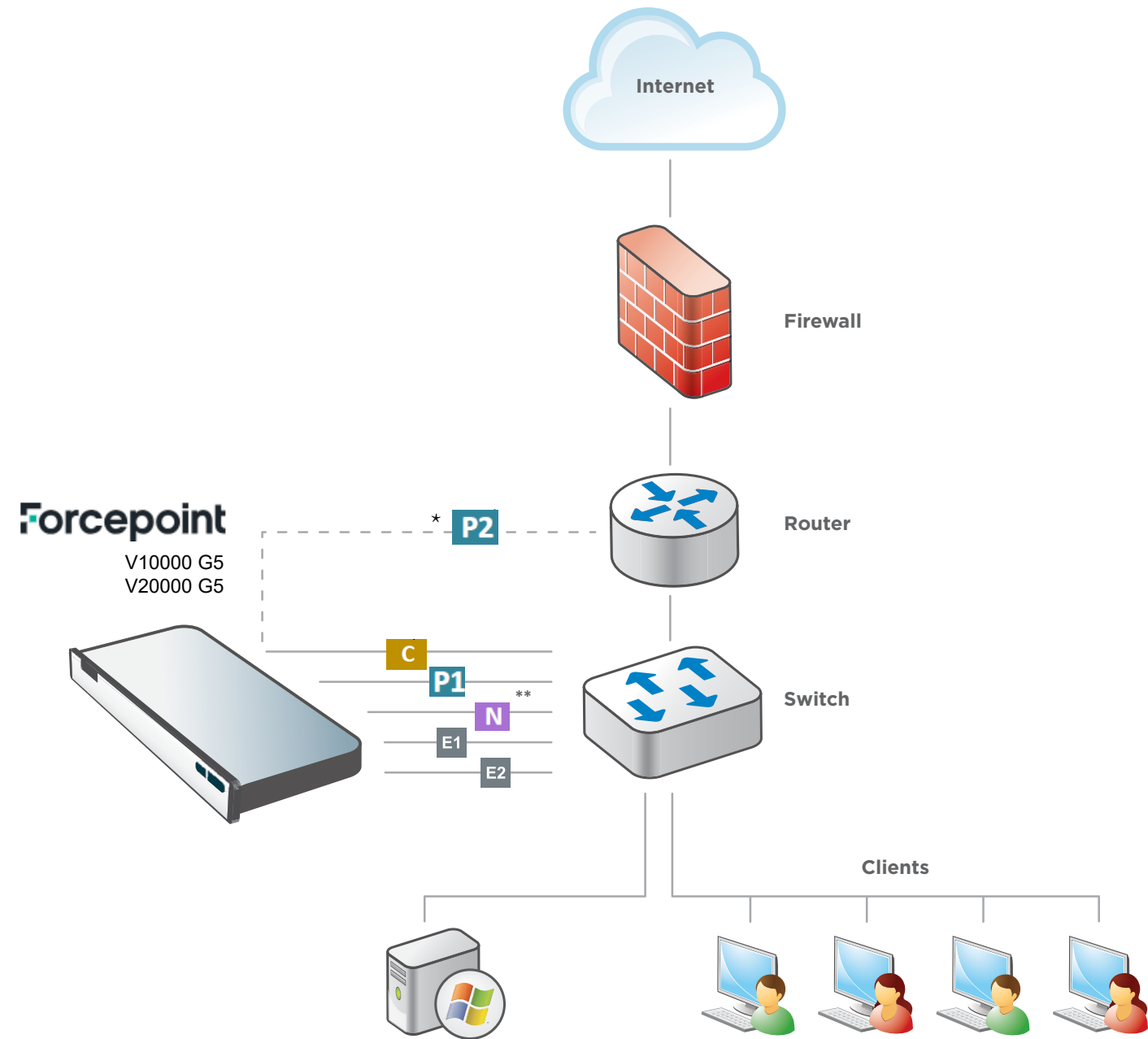
### Email Mode

#### 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.

## 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/s/article/V-X-and-I-Series-Appliances-Documentation](https://support.forcepoint.com/s/article/V-X-and-I-Series-Appliances-Documentation)

Online Support and Contact Information

<https://support.forcepoint.com/s/contactsupport>

## Deployment Reference Sheet

### Appliance Information

C Interface IP:

Hostname:

*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:

#### Forcepoint Email/Web Security Interfaces - P1 P2

P1 Address:

Default Gateway:

Subnet Mask:

Primary DNS:

P2 Address:

Secondary DNS:

Subnet Mask:

Tertiary DNS:

#### Network Agent Interface - N

IP Address:

Primary DNS:

Subnet Mask:

Secondary DNS:

Default Gateway:

Tertiary DNS:

#### NIC Teaming Failover - E1 E2

##### E1 (Bonded with P1)

IP Address:

Default Gateway:

Subnet Mask:

Primary DNS:

##### E2 (Bonded with P2)

IP Address:

Secondary DNS:

Subnet Mask:

Tertiary DNS:

### Forcepoint Security Manager

#### Web

Policy Server IP:

Log Server IP:

Subscription Key:

#### Email

Log Server IP:

Authentication Mode:

#### SQL Server

IP Address:

User Name:

Password:

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