

# Quick Start Guide

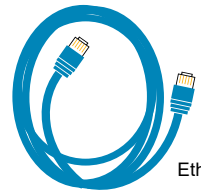
## Forcepoint V5000 G5 Web or Email Security Appliance



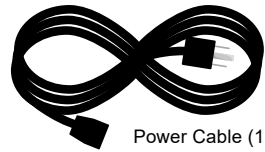
### Before you begin...

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 (1)



Bezel (faceplate)

### Static Ready Rail Kit



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



Contact Forcepoint Technical Support if any items are missing.

## 2 Rack Appliance

To mount the V5000 appliance, use the Static Ready Rail Kit provided.

See the Rack Installation Instructions included in the Static Ready Rail Kit for more details.



## 3 Determine Security Mode

The appliance supports the following security modes:

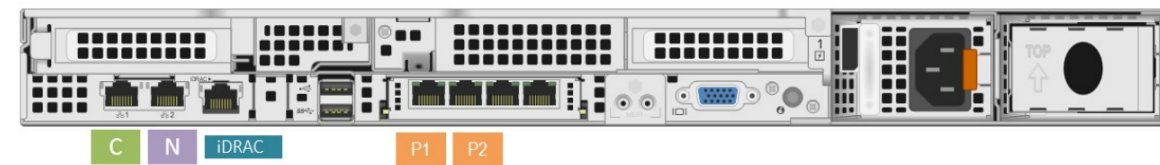
- **Web** (Forcepoint Web Security or Forcepoint URL Filtering)
- **Email** (Forcepoint Email Security)

Based on your subscription, select 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.*

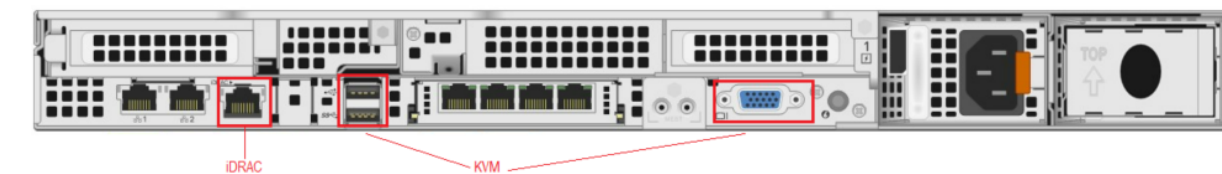
	Web	Email
Required Ports:	C P1 N	C P1
Optional Ports:	P2 iDRAC	P2 iDRAC



Interface	Function
C	. Provides communication with other Forcepoint components, including Forcepoint Security Manager. . Handles database downloads from Internet.
P1	<b>Web mode:</b> . Enables Content Gateway proxy to receive Internet requests and communicate with web servers.
P2	<b>Email mode:</b> . 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. . Connects to switch port. If sending blocking information through N, connect to bidirectional span, monitor, or mirror port on switch.
iDRAC	. Allows remote management. . Preferred method for managing the server. . See Knowledge base Article #11964 for more information.

## 5 Connect Input Device & Power On

Connect to the appliance via Virtual Console feature of iDRAC or directly via KVM in order to access the command line interface for initial configuration.



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.

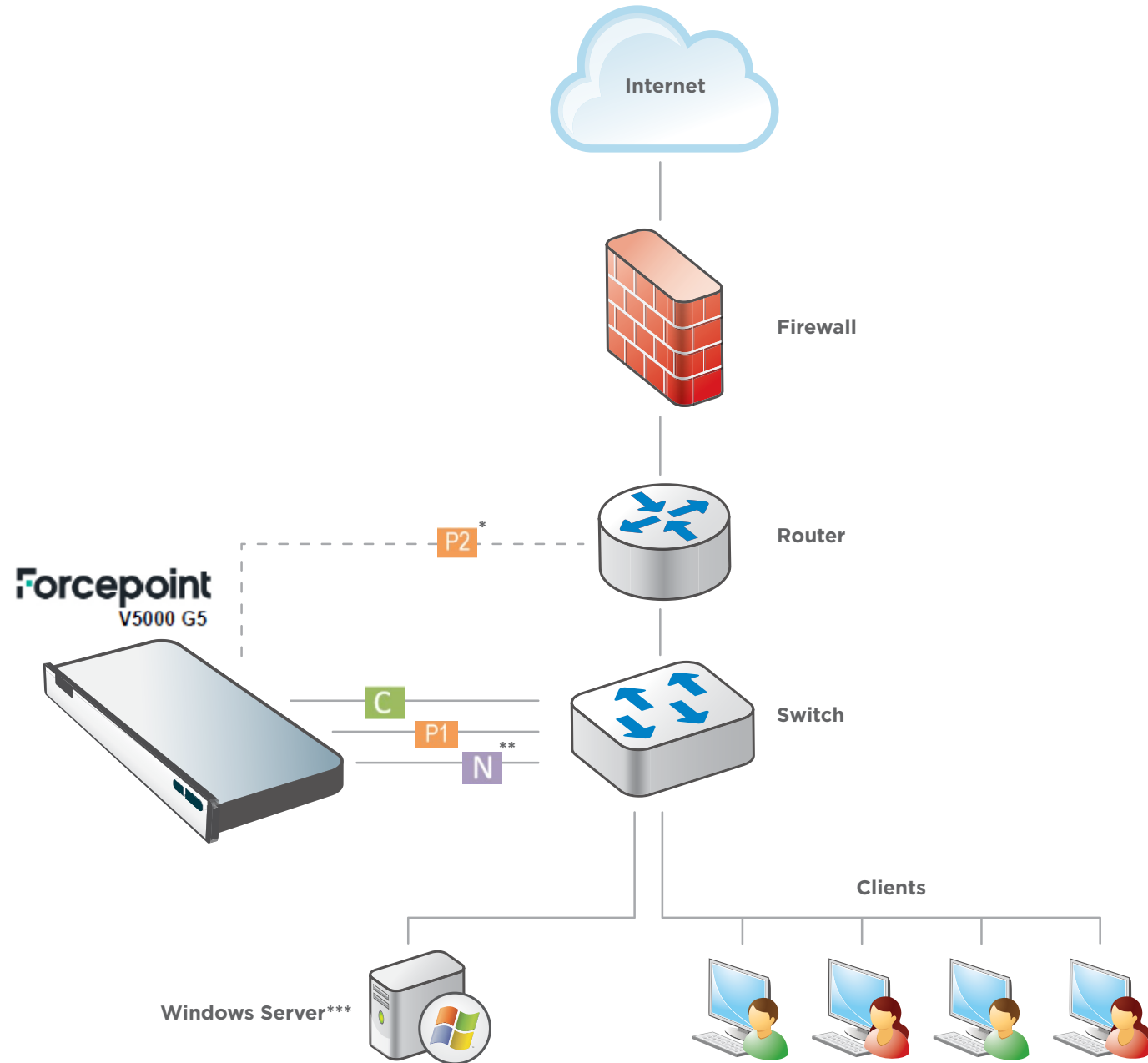
### Email Mode

#### 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).

## Appliance Deployment Overview

You can deploy one or more appliances on your network. The diagram below illustrates a basic appliance deployment. A separate host with Windows Server is required for running Forcepoint Security Manager.



\* 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.

## 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:

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 Security Manager

#### Web

Policy Server IP:

Log Server IP:

Subscription Key:

#### Email

Log Server IP:

Authentication Mode:

#### SQL Server

IP Address:

User Name:

Password:

## Support & Resources

Getting Started Guide

[http://www.websense.com/content/support/library/appliance/v85/getting\\_started/getting\\_started.pdf](http://www.websense.com/content/support/library/appliance/v85/getting_started/getting_started.pdf)

Online Support and Contact Information

[support.forcepoint.com/s/contactsupport](http://support.forcepoint.com/s/contactsupport)