SOLUTION BRIEF

Using FortiDeploy for Fast and Easy Deployment of Fortinet NGFWs and APs

Executive Overview

Security IT resources continue to be strained due to a lack of available skilled staff to fill positions. At a time when many security architectures are growing to keep up with a rapidly expanding attack surface and ever-evolving advanced threat landscape, IT and security leaders are often expected to keep up with risk exposures without a full team of players. The FortiDeploy feature allows for simplified import and at-scale provisioning of FortiGate next-generation firewalls (NGFWs) and FortiAP access points (APs). Integrated as part of FortiManager, FortiGate Cloud, and FortiAP Cloud management tools, FortiDeploy allows administrators to deploy local or remote installed Fortinet NGFWs and APs to their preferred management interface with a few clicks of the mouse.

Today's networks are increasingly dispersed. Normal mergers and acquisitions, adding branch offices, or even simple business growth that includes adopting private or public cloud services extend the reach of the network—and subsequently, the network attack surface. Threats targeting businesses are growing in number and sophistication, looking to exploit any and all weaknesses they can find in network defenses. At the same time, businesses of all sizes and industries are struggling to keep their IT security teams fully staffed due to historic skills shortages. Security administrators need tools to help them do more with less.

The shortage of cybersecurity professionals has grown to nearly 3 million unfilled positions around the world—with roughly 500,000 of those coming from North America.[1]

Zero-Touch Provisioning with FortiDeploy

In the management world, zero-touch provisioning has revolutionized onboarding and provisioning. Rather than use command-line interfaces (CLI) to configure devices one at a time, administrators can use the Fortinet FortiDeploy feature to automate the rollout of devices all at once while enabling the manageability of those with a single click.

FortiDeploy enables deployment of security and wireless infrastructure both locally and at remote locations where onsite provisioning technical expertise is limited. Deployment settings can be preconfigured—such as assigning a device to a specific FortiGate Cloud, FortiAP Cloud, or FortiManager for reporting. Deployed devices can then automatically find their intended management interface with no onsite IT involvement.

Connecting FortiDeploy to FortiGate and FortiAP

When a Fortinet customer includes FortiDeploy on their Fortinet device order (e.g., FortiGate NGFWs, FortiAP), they receive a bulk deployment FortiCloud key tied to all supported devices within that order. When the customer visits their FortiGate Cloud or FortiAP Cloud management console, they can enter either the key for a single device or the bulk key for all devices sent with their order.

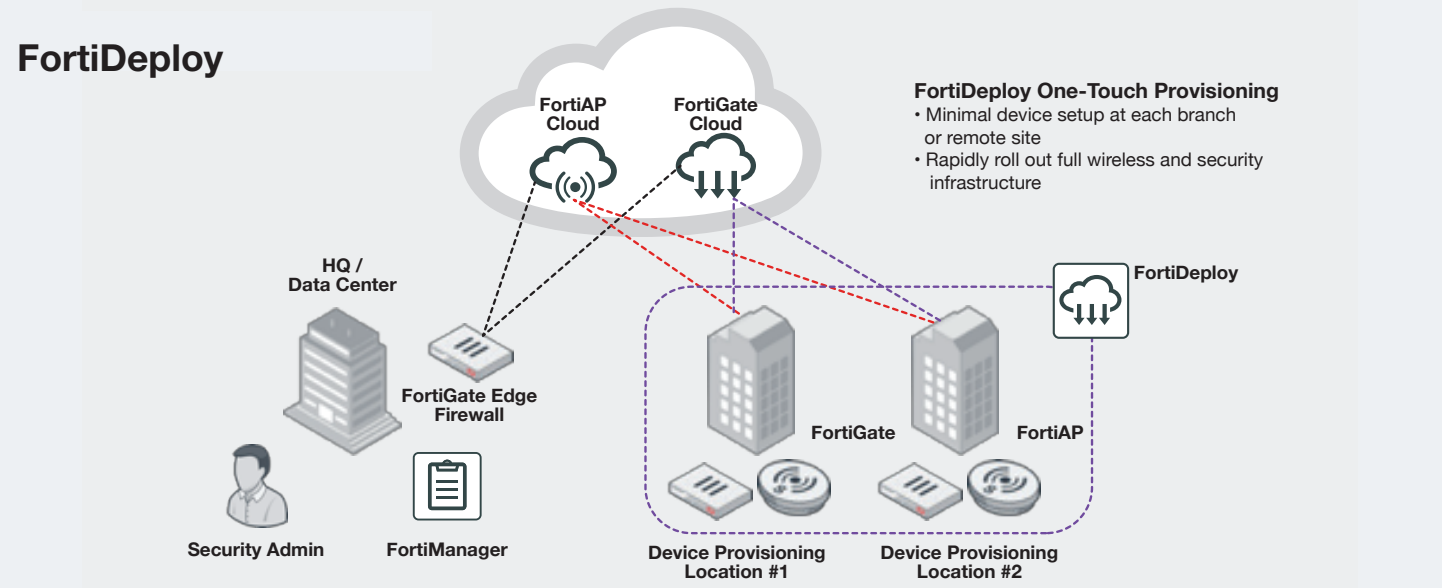
Upon entering the key, the full list of device serial numbers are listed in the management portal. As devices are plugged in at their respective remote locations, FortiDeploy automatically obtains an IP address via DHCP. These devices then "call home" to FortiGate Cloud or FortiAP Cloud. The device then receives the customer's preconfigured management information for these devices. When this process is complete, the devices can be monitored and managed from the chosen Fortinet management interface.

Mapping Supported Devices

Bulk FortiDeploy keys can be created to include all FortiAP and FortiWiFi devices as well as smaller FortiGate models that include a dedicated wide-area network (WAN) port (up to and including the 200E). Any combination of these devices can be included in a single-key deployment.

[1] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)2, October 18, 2018.

When assigning options for management and control, a FortiGate or FortiWiFi device can be assigned to a specific FortiManager or FortiGate Cloud. FortiAP devices can be assigned to FortiManager, FortiAP Cloud, or to a specific FortiGate.



Remote Provisioning with Multi-tenancy for MSPs and MSSPs

When coupled with multi-tenancy, FortiDeploy allows managed service providers (MSPs) and managed security service providers (MSSPs) to add FortiGate and FortiAP devices en masse to their FortiGate Cloud or FortiAP Cloud accounts. From there, the multi-tenancy feature of FortiDeploy allows administrators to select a configuration template and operating system version (FortiOS) to deploy with the newly added devices.

Key Benefits of FortiDeploy

Activity	Challenge	FortiDeploy Benefits
Activation and Onboarding	Security devices must be deployed at branch offices by field technicians who do not have specialized training. However, security management is handled at HQ.	■ Easy and secure onboarding of Fortinet NGFWs and APs via Fortinet management platforms ■ Reduced time to add a device by automating the process for plug-and-play configuration ■ New device installations do not require highly technical personnel for configuration, but rather can be performed remotely from the cloud
Centralized Device Management	Security administrator must provision and install policies centrally	■ Centralized management from a single web-based console (deployment and undeployment of devices in bulk) ■ Flexible and scalable to quickly meet business demands

Summary: Simplified Security Management That Saves Resources

FortiDeploy automates device deployments and supports single-click manageability of firewalls, access points, and other security solutions across today's increasingly distributed network architectures. Businesses of all sizes with multiple devices to provision can ensure consistent security across their organization while reducing the burden on limited staff resources.

FORTINET

www.fortinet.com

February 26, 2019 9:56 AM

349864-0-0-EN

Macintosh HD:Users:ckluck:Documents:FORTINET_ck:2019:FortiDeploy-sb:FortiDeploy-sb