DEPLOYMENT GUIDE

Fortinet Security and Centrify

Fortinet Security and Centrify

Overview

Fortinet network security appliances and subscription services provide broad, integrated, and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Fortinet offers a flexible, end-to-end solution that incorporates

wireless and wired access, security, authentication, switching, and management in an easily managed system that allows systemwide policy enforcement. Centrify offers secure, single sign-on for cloud and mobile applications, as well as management of a broad variety of mobile devices, enabling enterprises to uniformly and efficiently manage identity and access policies for cloud and mobile resources combined with Fortinet`s enterprise security. This provides the customer with the combined benefits of both on-premises and cloud-based unified identity services and enterprise security.

Deployment Prerequisites

The Fortinet and Centrify deployment requires the following:

1. FortiGate Firewall
2. Network AD Server
3. Client Device connecting to the network
4. Centrify Software or Cloud Account

Architecture Overview

The following diagram illustrates the various services and components that are part of the Fortinet Centrify integration. Some of these Centrify services are delivered in the Centrify Cloud. This includes a FortiGate appliance and the Centrify Identity Platform, which provide the underlying infrastructure for the Centrify Identity Service and the Centrify Privilege Service. These cloud services are hosted on the Microsoft Azure Platform-as-a-Service and operated by Centrify.

Centrify also offers solutions such as Centrify Server Suite, which runs as a set of on-premises software services that provide direct integration with Microsoft Active Directory or LDAP directory services. The Centrify Cloud Connector acts as a secure connection between various on-premises services and the Centrify Cloud Services. Centrify, along with Fortinet, can provide secure identity management services across both on-premises platforms and mobile devices.

The Identity Platform can be used with existing Active Directory, LDAP infrastructures, or use Centrify's cloud-based directory or both.

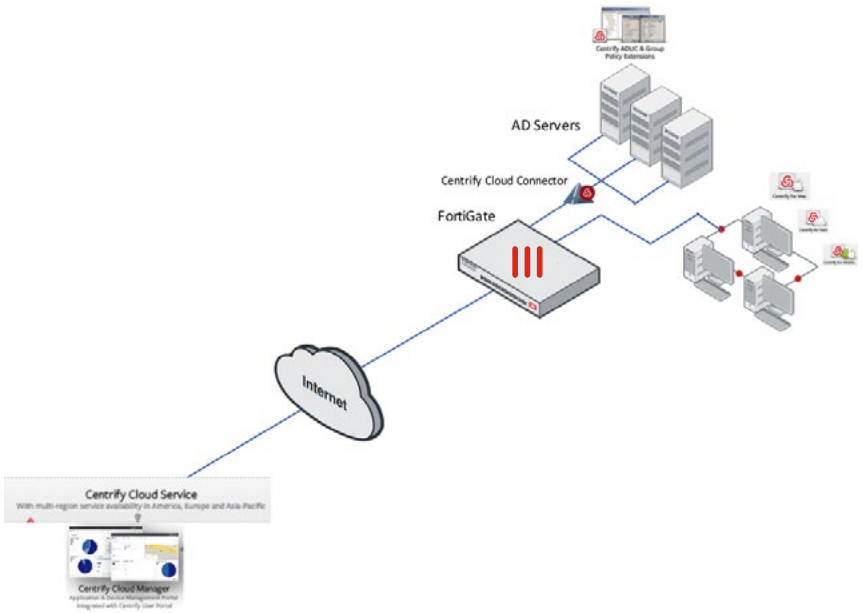

Figure 1: Topology

Partner Configuration

Centrify Cloud

For customers who want to integrate the Centrify Cloud with their on-premises Active Directory or LDAP directory for user authentication, the Centrify-supplied software program called the Centrify Cloud Connector needs to be installed inside their environment. The Centrify Cloud Connector is a simple Windows service that runs behind a customer's firewall to provide real-time authentication, policy, and access to user profiles without synchronizing data to the cloud.

The Cloud Connector seamlessly integrates with Active Directory or LDAP without opening extra ports in an organization's firewall or adding devices in their DMZ, and it acts as a gateway for access to on-premises applications without the need for VPN.

When the Cloud Connector starts up, it creates a persistent, outbound connection over port 443 (https) to connect to the Azure cloud via the Microsoft Service Bus API. Traffic is encrypted and mutually authenticated (a "secure channel") between the Cloud Connector and the cloud tenant.

First complete registration with Centrify. Log in to Centrify and download the Cloud Connector. Steps to installing Centrify Cloud Connector:

1. Log on to the Centrify Cloud Manager at http://cloud.centrify.com/manage.
2. Click on Settings → Network.
3. Click on Add Centrify Connector.
4. Click Download and install it on your Windows AD server. See Figure 2.
5. Use Portal Credentials for user with "Register Proxies" rights to integrate your Active Directory with Centrify Cloud Services. See Figure 3.

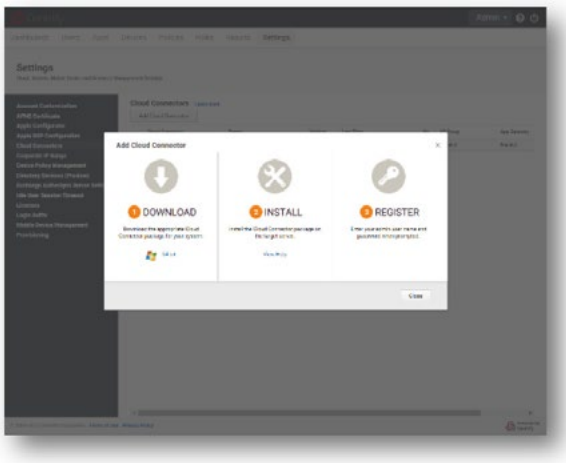

Figure 2: Connectors Download.

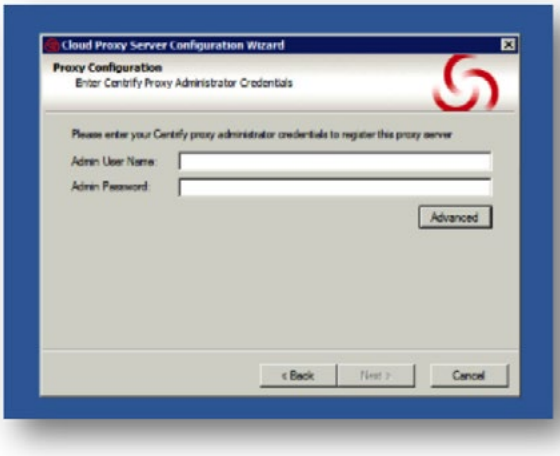

Figure 3: Connector Login.

On the Centrify Admin Portal, you should be able to see your server integrated and the status as active. This can be visible under Settings > Centrify Connectors. See Figure 4 below.

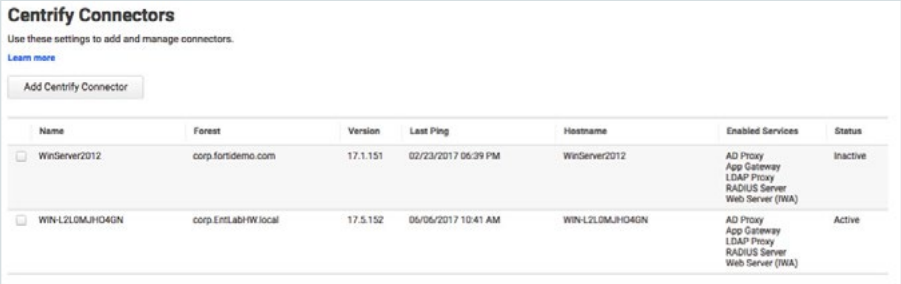

Figure 4: Connectors Configured

The next step is to add Users. Click Core Services > User and Add User. You can also bulk import users. Figure 5 below shows how to import users from the AD server.

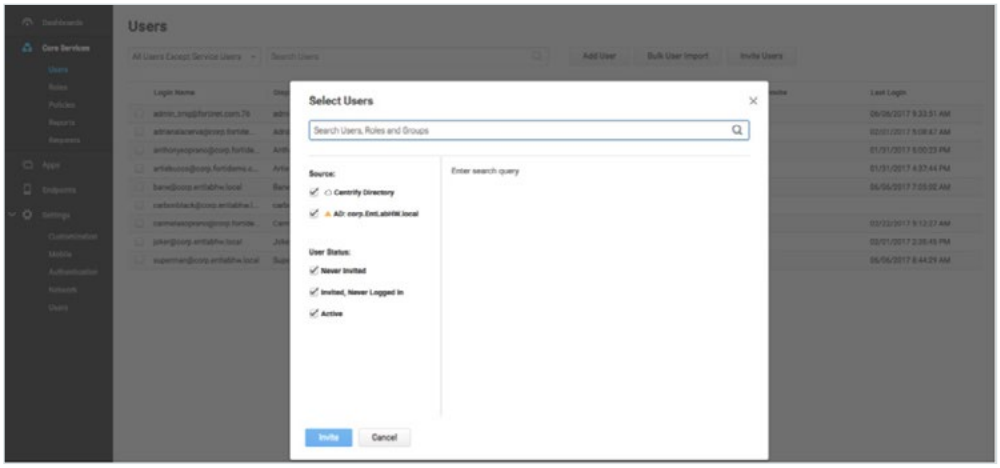

Figure 5: Adding Users.

You can also import the roles from the AD server or manually create roles as shown below.

Figure 6: Adding Roles.

Centrify Cloud Manager provides Mobile Device Management with FortiGate and FortiAP.

You can centrally configure security and access policies for all wired and wireless users. You can centrally manage devices (info, lock, wipe) and Fortinet App directly to the mobile devices from Centrify.

Fortinet Configuration

For this MDM integration, there is no requirement to configure the FortiGate device.

Fortinet RADIUS Authentication

For RADIUS Authentication, FortiGate can be configured to work with Centrify Cloud as an external RADIUS Server.

Mobile Device Configuration

Install and launch the Centrify application on the mobile device. The user account gets verified against Centrify Cloud Service.

Dashboard and Reporting

The dashboard gives an overview of the login attempts, security events, locations, and devices in the network, as shown in the figure below.

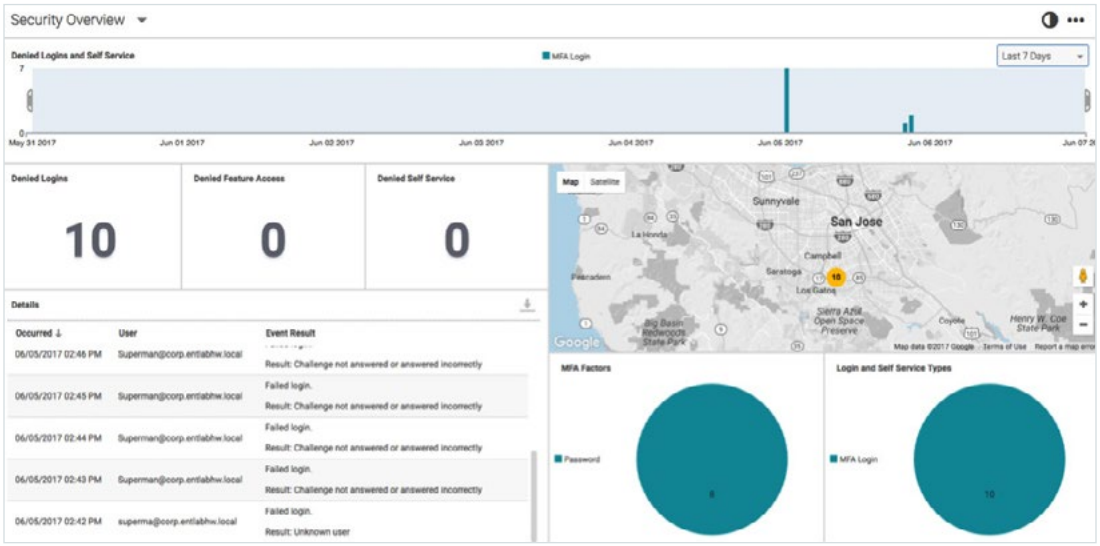

Figure 7: Dashboard.

The Users tab under Core Services lists the status of the authorized users.

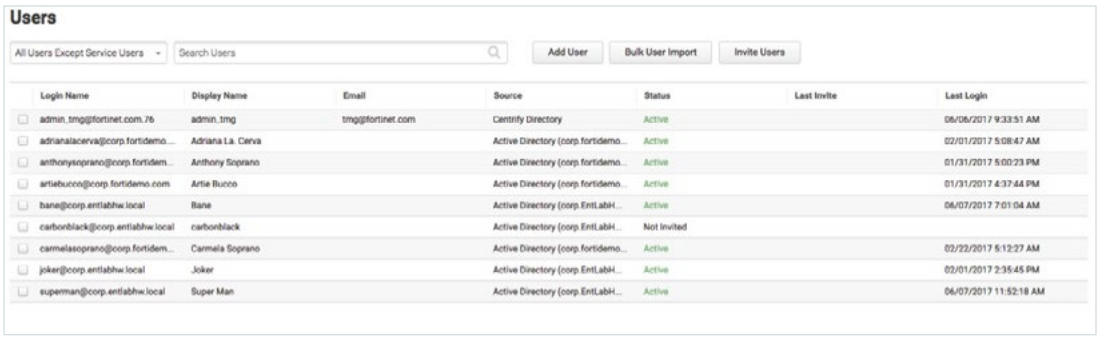

Figure 8: User.

The Apps tab lists the apps that can be deployed and the status of those apps.

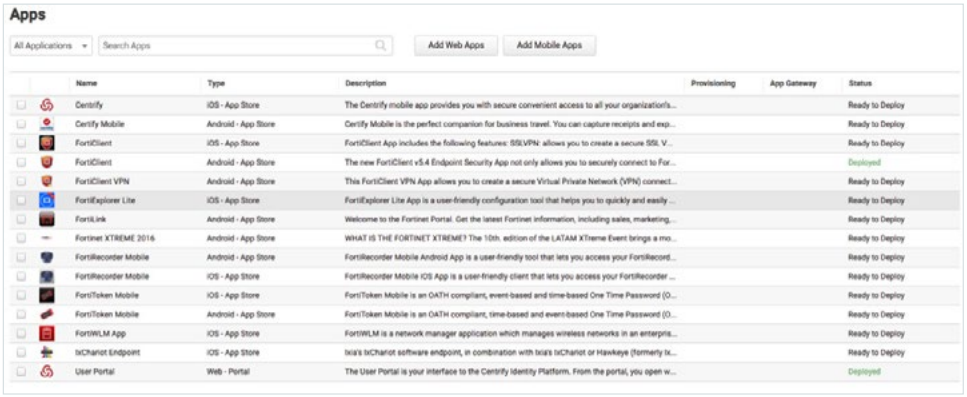

Figure 7: Dashboard.

The Endpoints tab lists the status of the authorized device, the apps installed, and details of the hardware, as shown below.

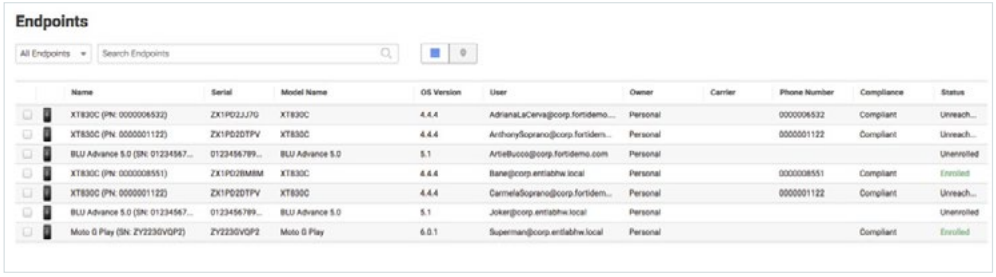

Figure 8: User.

Summary

Access to Centrify Demo: This demo is part of FortiDemo and EntLab portal and can be accessed using https://aap0764.my.centrify.com/. Log in as admin/admin.

How To Get Help

Fortinet:

This demo is part of the EntLab portal. Contact the Technical Marketing Group to access the setup.

- https://fuse.fortinet.com/p/do/sd/sid=2302&fid=3542&req=direct
- tmg@fortinet.com

Centrify:

- https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Fortinet-Centrify.pdf
- http://community.centrify.com/centrify/attachments/centrify/techblog/537/1/Centrify%20for%20Fortinet%20RADIUS%20configuration%20guide.pdf
- support@centrify.com

September 14, 2021 3:38 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 2:DG-Fortinet Security and Centrify:DG-Fortinet Security and Centrify_2021

89094-A-A-EN