JUNOS PULSE APPCONNECT

A Micro VPN That Allows Specific Applications on Mobile Devices to Independently Leverage the Connect Secure Gateway
# Table of Contents

- Executive Summary ................................................................. 3
- Introduction .................................................................................. 3
- Prerequisites .................................................................................. 3
- Technical Details ........................................................................... 3
- Connect Secure Gateway Configuration ........................................ 4
- Deployment Models ....................................................................... 5
- iOS 7 Per-App VPN ........................................................................ 5
- MobileIron Deployment (iOS 7 only) ............................................. 6
- AirWatch Deployment (iOS 7 only) ................................................ 7
- Samsung KNOX ........................................................................... 9
- AppConnect SDK ......................................................................... 9
- PAC License .................................................................................. 9
- Conclusion ..................................................................................... 9
- About Juniper Networks ............................................................... 10
Executive Summary

Juniper Networks® Junos® Pulse AppConnect is a micro VPN solution that runs on mobile devices (iOS and Android) to enable encrypted communications between specific applications (via AppConnect tunnels) and a Juniper Networks Junos Pulse Connect Secure gateway (Juniper Networks SA Series SSL VPN Appliances or MAG Series Junos Pulse gateways, formerly Junos Pulse Secure Access Service or SSL VPN). It allows enterprise-level IT administrators to secure sensitive data transactions between remote mobile devices and the enterprise network. Unlike a standard Layer 3 VPN, the administrator has some discretion as to which applications leverage the AppConnect tunnel. This creates an environment where only sensitive enterprise data travel back to the enterprise network, leaving all nonsensitive (personal) data to travel over standard data paths from the device to the Internet.

Introduction

There are three core deployment models, each with specific use cases and requirements. The deployment models are:

1) iOS 7 Per-App VPN (requires third-party MDM solution to deploy)
2) Samsung KNOX VPN
3) AppConnect SDK

While AppConnect is a software-based solution installed on mobile devices, it requires Connect Secure hardware or a virtualized Connect Secure environment in order to terminate AppConnect tunnels, as well as an enablement license, called a PAC license (Pulse AppConnect license), for each physical device that does accept AppConnect tunnels from mobile devices. Virtual Connect Secure deployments do not currently require the PAC license.

Depending on the deployment model, additional third-party solutions might be required. Such solutions include MobileIron, AirWatch, or any other MDM solution that allows the administrator to define and deploy iOS 7 Per-App VPN settings. Such third-party MDM solutions can also be directly integrated with newer versions of the Connect Secure (version 8.x or later), allowing even more control over access policies for mobile devices. This creates a robust and secure environment where mobile devices can be trusted to remotely access and leverage sensitive enterprise data located on the enterprise network.

Prerequisites

The deployment model that best suits a given enterprise is defined by a few simple questions.

1) Do you deploy managed or proprietary mobile applications?
   a. Yes—All three deployment models can be leveraged to secure data transactions of managed or proprietary applications.
   b. No—Samsung KNOX can still be used to secure data transactions of KNOX-based applications, and iOS 7 Per-App VPN can still be used to secure the Safari browser. The AppConnect SDK cannot be leveraged.

2) Do you have an existing MDM deployment that supports iOS 7 Per-App VPN settings?
   a. Yes—The iOS7 deployment model can be leveraged.
   b. No—Only the KNOX or AppConnect SDK deployment models can be leveraged.

3) Do you have existing Connect Secure Gateway(s)? (SA Series or MAG Series hardware or a virtualized Connect Secure environment, software version 7.2 or later)
   a. Yes—You need to add a PAC license to each physical gateway in order to accept AppConnect tunnels.
   b. No—The AppConnect solution cannot be deployed in any fashion. You must purchase a MAG appliance or virtual appliance to terminate AppConnect tunnels.

Technical Details

AppConnect tunnels leverage WSAM technology on the Connect Secure gateway. There are settings that must be configured on the gateway in order for mobile devices to leverage WSAM. AppConnect tunnels consume one concurrent session/license per AppConnect tunnel. The number of concurrent licenses a single device can, or does, consume differs based on the implementation, deployment, and use case of the AppConnect tunnels. The gateway must be running software version 7.2 or later. In situations where multiple connections are opened between a device and the Connect Secure Gateway, connection limits are 124 per device (Connect Secure version 8.0R3 and later, 64 connections per device for earlier versions of the Connect Secure Gateway).
Connect Secure Gateway Configuration
The following is a step-by-step guide showing how to configure the Connect Secure gateway. The administrator creates a user realm and role(s), defines role mapping, creates a sign-in policy, and enables the WSAM and VPN settings. Optionally, MobileIron or AirWatch MDM servers can be linked to the SA Series to allow additional Host Checker rules. More details regarding MobileIron and AirWatch integration into the Connect Secure gateway can be found here.

1) Create a new User Realm. Optional: Device Attributes.

2) Optional: Create a new sign-in URL to be used when connecting a mobile device via AppConnect.

3) Add the newly created user realm to the selected realms list.
4) Define role-mapping options for the realm.

5) Turn on WSAM and VPN tunneling in the role(s) used for AppConnect-enabled devices.

Deployment Models

There are three core deployment models, each with specific use cases and requirements. The deployment models are iOS 7 Per-App VPN, Samsung KNOX VPN, and AppConnect SDK. Additionally, the iOS 7 Per-App VPN deployment model also requires the use of a third-party MDM provider.

iOS 7 Per-App VPN

Apple has created a set of MDM APIs, referred to as iOS 7 Per-App VPN, and opened them up to MDM providers. These settings allow a device administrator to define a list of applications that leverage a VPN. This differs from previous versions of the Apple MDM VPN APIs. Previously, an administrator could only define a device-wide (Layer 3) VPN. Now, in iOS 7, not only can the administrator define a VPN connection, but the administrator can also define which managed applications have access to the VPN. This leaves all personal or nonsensitive applications (as defined by the administrator) to connect to the Internet directly, without the use of the VPN. As with all other Apple MDM APIs, the administrator must leverage an MDM provider to push and manage these settings on the end user’s iOS device.

In the case of iOS 7, the Juniper Networks Junos Pulse application (version 5.0R4 or later) must be installed on the end user’s device for the device OS to be able to open AppConnect tunnels terminating on a Connect Secure gateway. The Junos Pulse application includes a system-level plug-in that is activated by the iOS 7 Per-App VPN settings. End users must open Junos Pulse and accept the End User License Agreement (EULA) to enable the plug-in.
Two main limitations are currently applied to applications that leverage the iOS 7 Per-App VPN. These limitations are created by Apple’s current implementation of the iOS 7 Per-App VPN APIs and are subject to change in any future iOS release. The limitations are not unique to Juniper’s implementations of AppConnect.

1) Only managed applications are able to leverage the iOS 7 Per-App VPN.
   a. A managed application is one that has been installed on the end user’s device via an MDM solution.
   b. In addition to managed applications, Safari can be forced over the AppConnect tunnel.
2) Only TCP is currently supported (UDP support is expected in a future release).
   a. UDP packets that travel over the iOS 7 Per-App VPN are dropped from the network stack by the system.
   b. Any application that sends data using the UDP protocol fails to function if added to the iOS7 Per-App VPN.

The deployment steps to enable iOS 7 Per-App VPN differ based on the currently deployed MDM solution. The following are two step-by-step examples of the most common MDM solutions, MobileIron and AirWatch.

**MobileIron Deployment (iOS 7 only)**

It is presumed that the administrator has a basic understanding of the MobileIron solution. For additional details, please refer to the MobileIron documentation. MobileIron requires an additional license to enable Per-App VPN settings. All details of integration are subject to change. This deployment is for MobileIron version VSP 5.9.2 Build 11.

1) Once logged in to the MobileIron server, navigate to Policies & Configs. Click on Add New in the drop-down menu and select VPN. MobileIron requires the use of certificate authentication. Optionally, the administrator can configure Safari Domains or VPN on Demand.

   ![MobileIron VPN Configuration](image)

2) After a VPN profile has been set up, the administrator can now apply the profile to individual managed applications. Navigate to the Apps tab, and change the “Selected Platform” to iOS. Selecting the edit option for a given application brings up settings for that application. Find the Per-App VPN setting and select the newly created VPN profile in the drop-down menu. Click Save. Repeat for each and every application that needs to send data over the VPN.
AirWatch Deployment (iOS 7 only)

It is presumed that the administrator has a basic understanding of the AirWatch solution. For additional details, please refer to the AirWatch documentation. All details of integration are subject to change. This deployment is for AirWatch version 7.1.

1) Log in to the AirWatch console and navigate to Devices, Profiles, List View, and select +Add. From here, select iOS and then VPN from the iOS drop-down menu.
2) Fill out the VPN profile and choose connection and authentication settings. Click Save.

3) Navigate to the Apps & Books tab. Locate each iOS application in a managed application list that needs to send data over the VPN, and edit the application settings. In the Deployment tab of the application settings, enable the Use VPN check box.
Samsung KNOX
Samsung KNOX is an enterprise-level application container offered by Samsung on select devices and firmware versions. Samsung KNOX enables the user to have a “dual persona” device. All personal applications and data reside outside the KNOX container. All sensitive enterprise applications and data reside inside the KNOX container. The KNOX container can be described as a virtual machine. All data and processes inside the container are only accessible from inside the container. Samsung has leveraged the AppConnect SDK to allow the device to pass all Internet communications that originate or terminate inside the KNOX container through a Connect Secure gateway via an AppConnect tunnel. Unlike iOS 7 Per-App VPN, the AppConnect tunnel is leveraged by the KNOX container, rather than individual applications. More details are expected to be provided when Samsung publicly releases the version of KNOX that includes AppConnect integration.

AppConnect SDK
The AppConnect SDK is a set of APIs and libraries, provided by Juniper, that allows mobile application developers to directly open socket-based SSL VPN connections to a Connect Secure Gateway. From the point of view of the Connect Secure Gateway, these tunnels mirror all other forms of AppConnect tunnels. The integration is done at the code level. Any application that integrates with the AppConnect SDK needs to be recompiled and manually deployed to the end users. The AppConnect SDK is best leveraged by container solutions or in-house applications that are deployed without the use of an MDM solution. The APIs include authentication and connection management functions. Connections can be shared across multiple applications on a single device. Contact your Juniper sales representative for more details regarding AppConnect SDK.

PAC License
The Pulse AppConnect (PAC) license is required for PAC feature enablement of mobile application-level VPN tunnel (also known as micro VPN tunnel) termination on SA Series and MAG Series SSL VPN gateways. AppConnect tunnels originate from applications running on an Android (4.x or later) or iOS (7 or later) mobile devices—for example, the iOS 7 Per-App VPN or Samsung KNOX feature configured by the MDM console, or a container that has fully integrated with the Junos Pulse AppConnect SDK. The AppConnect tunnels limit traffic to only approved applications, which is different from the standard Junos Pulse Layer 3 device-level VPN tunnel where all the traffic is sent over a VPN tunnel. An AppConnect tunnel consumes one concurrent session/license, up to the concurrent licenses available. The number of concurrent licenses a single device can, or does, consume differs based on the implementation, deployment, and use case of the application-level VPN tunnels. The PAC feature is interoperable with 7.x and 8.x software versions. The PAC license is not required on the virtual appliance. PAC functionality is automatically enabled on the virtual appliance. The PAC license is perpetual. Subscription PAC license are not available. A PAC license is needed on each gateway (standalone or in an active/passive cluster).

Conclusion
The three deployment models for Pulse AppConnect give administrators the ability to ensure the most common mobile devices (iOS and Android) can open AppConnect tunnels that terminate on a Juniper Networks Junos Pulse Connect Secure gateway. A PAC license is required when terminating AppConnect tunnels on a physical gateway. Some environments require the use of third-party MDM software. Deploying Pulse AppConnect ensures sensitive enterprise data are protected while leaving end-users personal data to travel over the standard path, limiting traffic on the enterprise network.
About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Copyright © 2014, Juniper Networks, Inc.