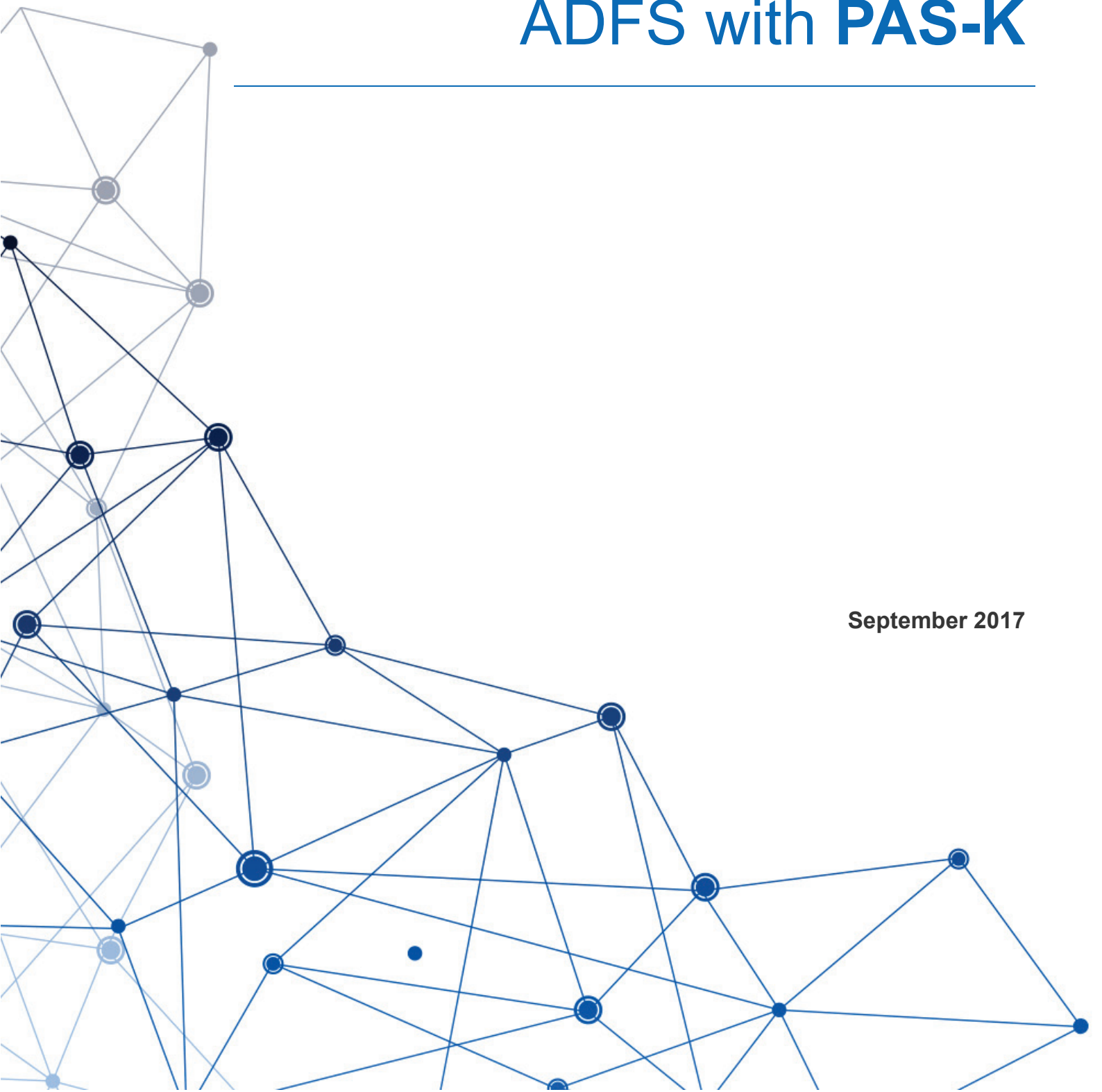

ADFS with **PAS-K**

September 2017



Overview

Active Directory Federation Services (ADFS) allows the sharing of identity authentication between two trusted partners beyond the boundary of an Active Directory (AD) forest. This feature is available within Windows Servers and provides users with Single Sign-On access to systems and applications across organizational boundaries. ADFS is becoming very popular due to the dramatic shift of enterprise customers towards cloud based services such as Microsoft Office 365.

ADFS enables use of existing AD credentials to access Office 365 or other trusted networks through AD federation. The benefit to users is a single access credential for access to applications. The single access credential works as long as the trust between the AD forests remains established.

Deployment Guide Overview

This guide describes how to deploy the PAS-K Series Application Delivery Controller (ADC)/Server Load Balancer in ADFS farms. This guide provides sections for the following deployment scenarios: Internal ADFS, and External Office365.

Architecture Overview

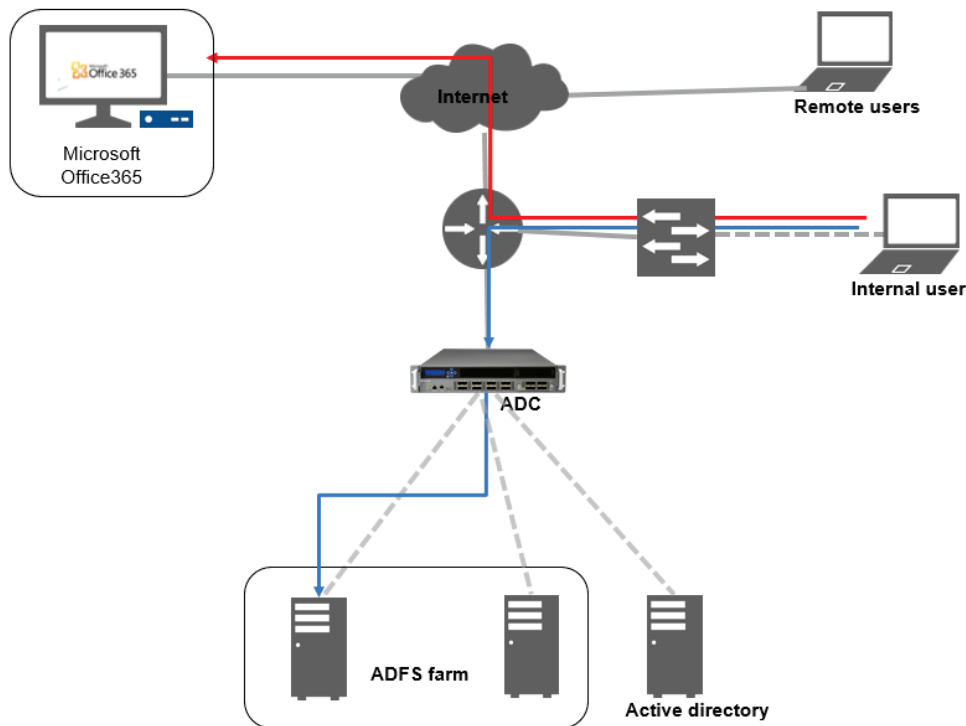


Figure 1 Logical configuration diagram: Using PAS-K

The following is the traffic flow for this scenario.

1. Both clients attempt to access the Office 365 resource;
2. Both clients are redirected to the resource's applicable federation service
3. Both clients are redirected to their organization's internal federation service;
4. The AD FS server authenticates the client to Active Directory;
5. Internal clients are load balanced directly to an AD FS server farm member;
6. Pre-authenticated to Active Directory via APM's customizable sign-on page;
7. Authenticated users are directed to an AD FS server farm member.
8. The AD FS server provides the client with an authorization cookie containing the signed security token and set of claims for the resource partner;
9. The client connects to the Microsoft Federation Gateway where the token and claims are verified. The Microsoft Federation Gateway provides the client with a new service token;
10. The client presents the new cookie with included service token to the Office 365 resource for access.

Summary and Conclusion

The PAS-K Series Application Delivery Controller enhances Microsoft Active Directory Federation Service (ADFS) by providing:

- High availability for ADFS servers to prevent downtime and access failure, with no adverse impact on user access to internal applications or Office 365 applications
- Provide seamless integration of Internal and External ADFS servers by load balancing requests, resulting in higher connection counts, faster end-user responsiveness and reduced ADFS application CPU utilization
- Seamless distribution of client traffic across multiple ADFS servers for site scalability
- Improved site performance and availability to end-users

Sample Configuration

1) Health check Configuration

```
health-check 1
  type tcp
  port 80
  apply
  exit
```

2) Real Server Configuration

```
real 1
  rip 1.1.1.101
  apply
  exit
```

3) Layer7 Pattern Configuration

```
layer7 pattern 1
  string /
  type uri
  match any
  apply
```

4) SSL Key Configuration

```
ssl key test_key
  mode generate
  type rsa
  length 1024
  encryption no
  apply
```

5) SSL Certificate Configuration

```
ssl certificate test_cer
  key test_key
  mode generate
  cname test.com
  country 81
```

6) SSL Profile Configuration

```
ssl profile 1
  certificate test_cer
  apply
```

7) SSL Profile Configuration

```
adv17slb test
  priority 100
  status enable
  ssl 1
  health-check 1
  vip 1.1.1.100 protocol http vport 80
  apply
  group test
    lb-method type rr
    real 1
    apply
  rule 1
    group test
    status enable
    pattern 1
    action group
```



About PIOLINK, Inc.

Specializes in the cloud data center optimization guaranteeing the best availability, performance, and security for applications also concentrating on agility and flexibility for data centers. We maximize customers' business in the fields of telecommunications services, financial services, public services, and corporations by providing various products and solutions for IT infrastructures such as data center operation, and managed security service

Visit: www.piolink.com | Contact: global@piolink.com

Depending on the product's upgrade and correction of printing errors, PIOLINK, Inc. reserves the right to change specifications at any time without notice. Actual products may vary due to product enhancement. Copyrights to the names of the companies and products on this document are the properties of those companies. For more information on how to order this product, please contact a local partner in your country, or use the following contact information.