

FortiADC Layer 7 Virtual Server with Kerberos Authentication Relay Deployment Guide

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



January 8, 2019

Layer 7 Virtual Server with Kerberos Authentication Relay Deployment Guide

TABLE OF CONTENTS

| | |
|---|----------|
| Change Log | 4 |
| Introduction | 5 |
| Overview | 6 |
| Example Topology description | 7 |
| Work flow | 8 |
| Configuration | 9 |

Change Log

| Date | Change Description |
|------------|--------------------|
| 2019-01-09 | Initial release. |

Introduction

This guide details the steps required to configure FortiADC Layer 7 Virtual Server with kerberos authentication relay based on V5.2 release.

Overview

Kerberos authentication is a computer authentication protocol that works on the basis of tickets (i.e., credentials). It provides several authentication choices, allowing nodes communicating over a non-secure network to verify each others' identity securely via a Key Distribution Center (KDC) and Service Tickets (STs). It is primarily used for client-server authentication model and provides mutual authentication by which both the client and the server verify each others' identity.

Kerberos authentication is built upon symmetric key cryptography and requires a trusted third party, and may also resort to the use of public-key cryptography in certain phases of the authentication process. By default, Kerberos Authentication Relay uses UDP port 88.

The Kerberos authentication consists of the following logical components:

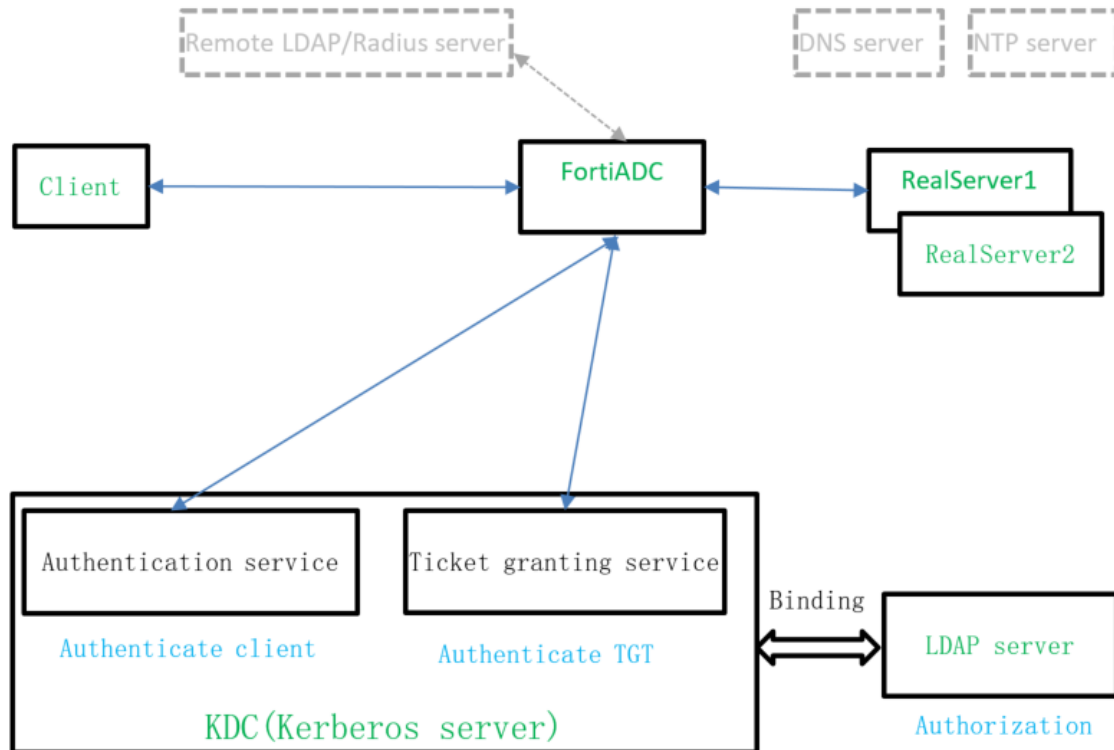
- Client
- Authentication Server (AS)
- Ticket Granting Server (TGS)
- Service Server (SS)

Often, the AS and TGS are located on the same physical server, i.e., the KDC.

If using Windows as authentication server, you will need to set up windows AD (Active Directory Domain services). Add proper Active directory users.

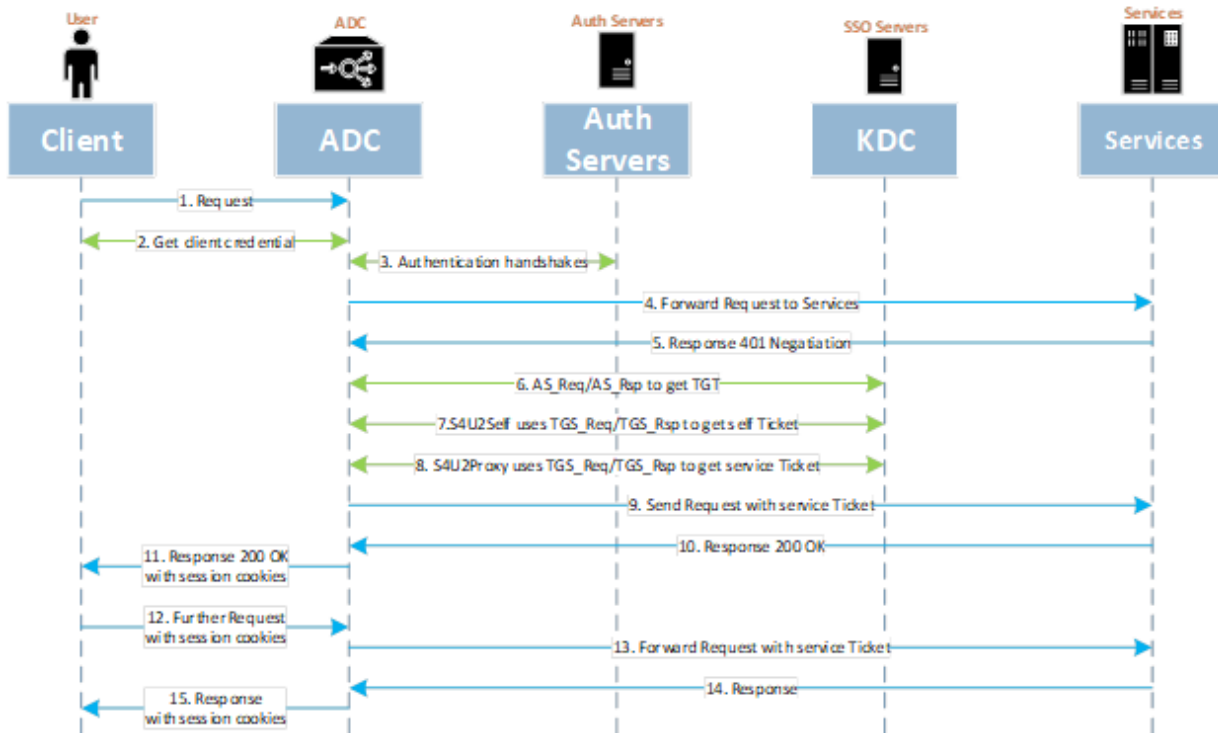
This deploy guide only provides configuration on the FortiADC. When on the Kerberos server setting, refer to the appropriate documents for the server that you chose.

Example Topology description



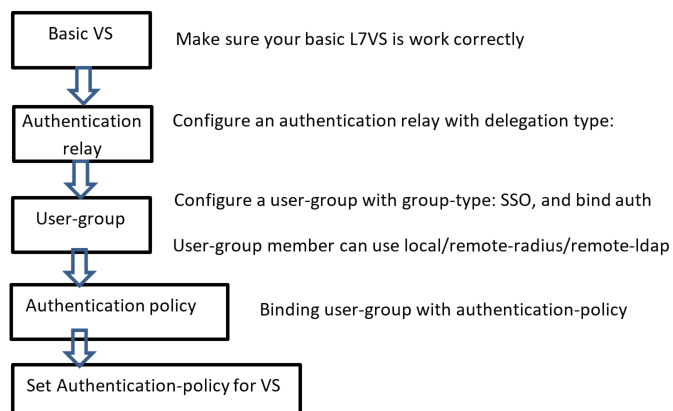
| server | hostname/IP example | note |
|--------------------|-----------------------|--|
| DNS server | | A DNS-server is needed, since all the tested domain name should be resolved by DNS server. Ignored in this guide, I will use local hosts file. |
| NTP server | | Kerberos is time aware of, so we need a NTP server to make sure all the devices in time consistency. Ignored in this guide, make sure the time is consistency in all the test machine. |
| Client | | We will test a HTTP service, so here we need a client which had http browser. |
| Remote LDAP/Radius | | Ignored in this guide, I will use FortiADC' local user for frontend authentication. |
| Kerberos server | kerberos.example.test | The Kerberos realm: EXAMPLE.TEST |
| Ldap server | ldap.example.test | The Base DN: dc=example,dc=test |
| VirtualServer | www218.example.test | |
| RealServer | | |

Work flow



Configuration

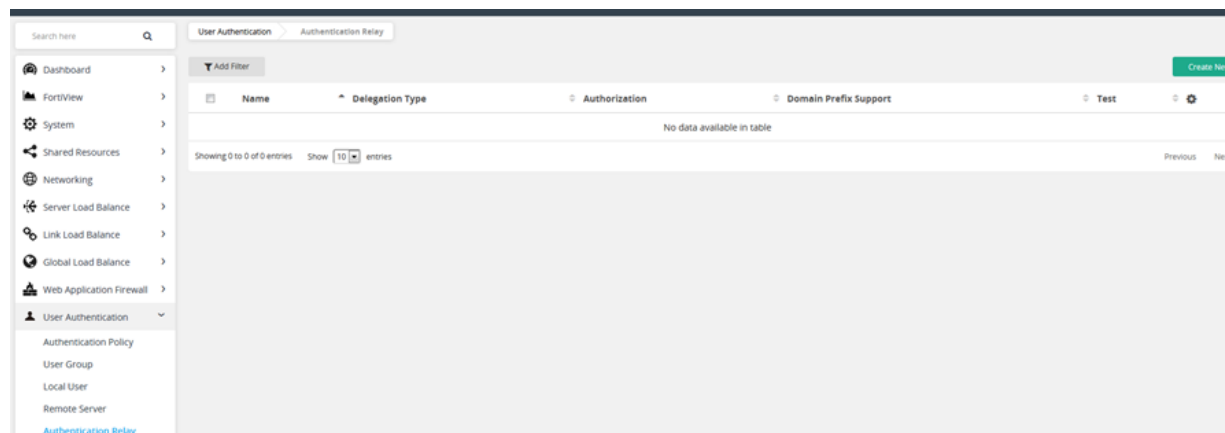
1. Overview



2. Set proper Layer 7 Virtual server

Configure a proper Layer 7 Virtual server and test it to make sure your Layer 7 Virtual server works properly.

3. Create a new authentication relay



Authentication Relay

Name
ker218

Delegation Type
 Kerberos HTTP Basic

KDC IP
Required. Specify the KDC IP.

KDC Port
88

Realm
EXAMPLE.TEST
Example: ADC.COM (Related with Delegated SPN)

Delegator Account
proxyadmin

Delegator Password
••••••••

Authorization
 HTTP Error 401 Always

Delegated SPN
HTTP/www218.example.test@EXAMPLE.TEST
Example: https/mail.adc.com@adc.com

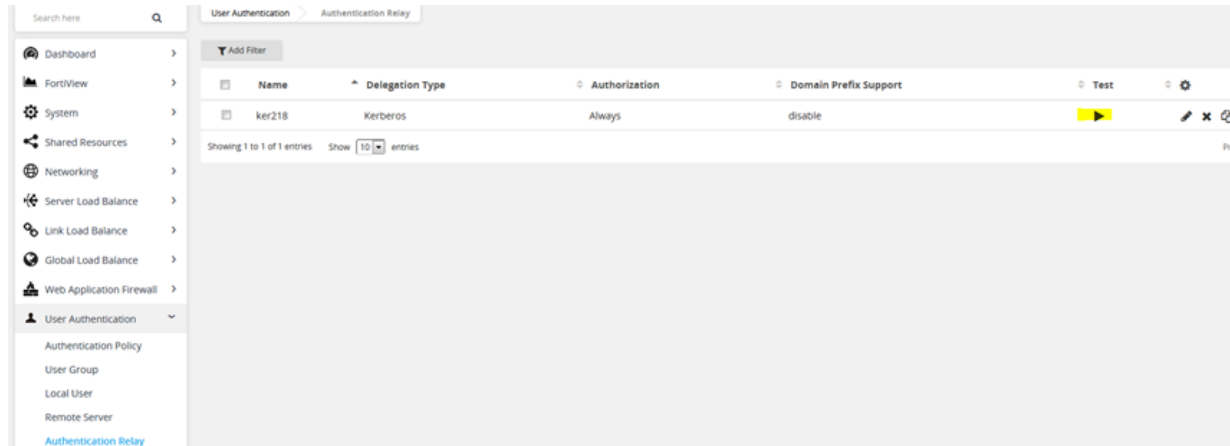
Domain Prefix Support
 OFF

- KDC IP: Enter the IP address of the KDC
- Realm: In most cases, your Kerberos realm is your domain name, in upper-case letters.
- The Delegator Account set on the ADC must match the account set on the LDAP/AD server. This account must have the delegation attribute on the LDAP/AD server and set the Delegated SPN.
 - For example, the Delegator Account here is: proxyadmin
 - For example, the Delegated SPN here is: HTTP/www218.example.test@EXAMPLE.test

- Delegated SPN (Service principal name): Specify the delegated SPN.

4. Test Kerberos authentication relay

After creating a Kerberos authentication relay you can test its setting by pressing the test button, and inputting the correct username for client. If the test fails, please check the Kerberos server setting.

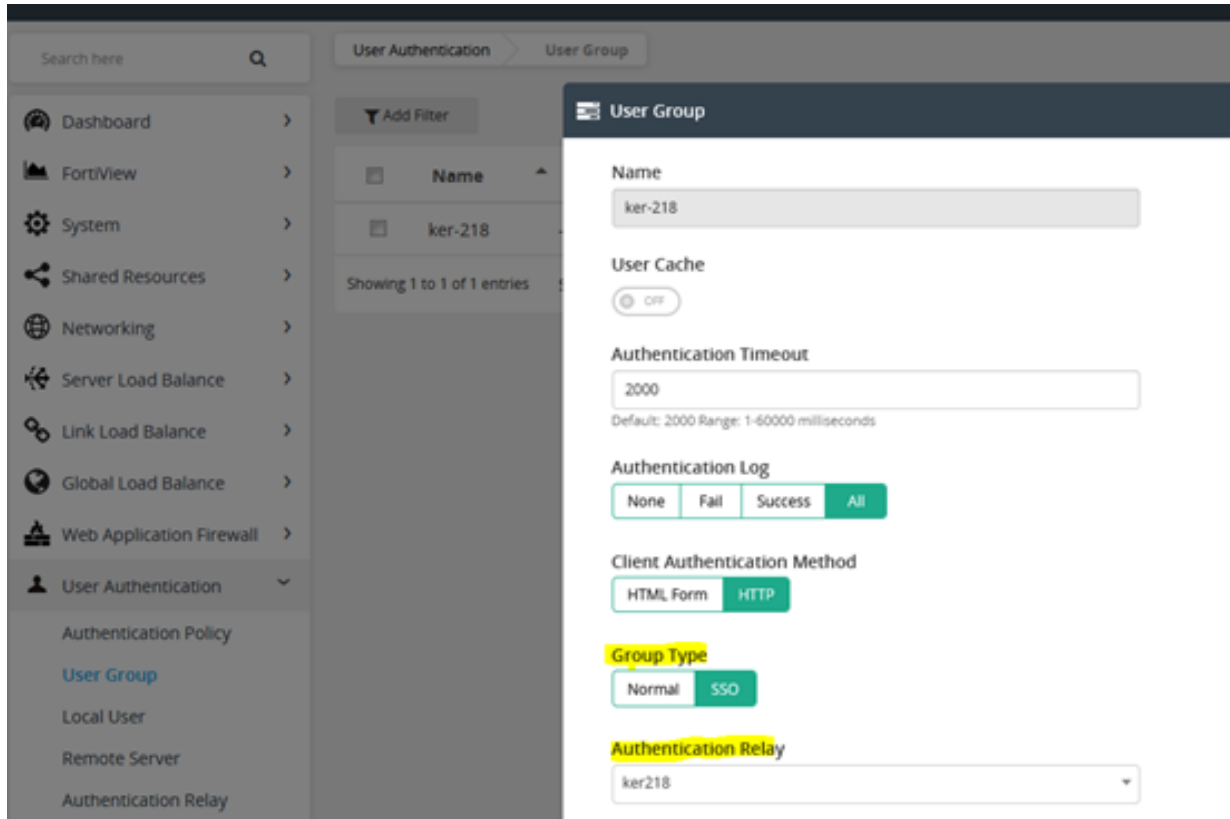


User Principle

Please provide a valid impersonated username

User

5. Create a user-group set group type to SSO and Authentication relay to kerberos



6. Add user group member

You can add preferred user group member for Virtual server authentication use. Here I use local Type.

☰ User Group

Authentication Relay

Authentication Session Timeout

SSO Support

Log Off URL

Member

▼ Add Filter Create New

| | ID | Type | Local User | LDAP Server | RADIUS Server | |
|--------------------------|----|-------|---------------------------|-------------|---------------|--|
| <input type="checkbox"/> | 1 | Local | adlocaluser_forcli ent | - | - | ⚙ ✎ ✕ 📄 |

When the client sends a http request to Virtual server, the FortiADC will ask the user to input a username and password. If the username and password match with the user-group member, the ADC will act as a proxy to authentication with Kerberos server by using the delegator account to get a self and service ticket.

☰ User Group

✎ Edit Member

Type

Local
LDAP
RADIUS

Local User

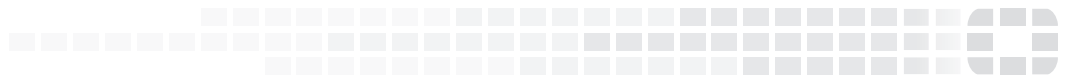
7. Set up authentication policy and bind it with Layer 7 HTTP(S) virtual server

The screenshot shows the Fortinet configuration interface for an Authentication Policy. On the left is a navigation menu with options like Dashboard, FortiView, System, Shared Resources, Networking, Server Load Balance, Link Load Balance, Global Load Balance, Web Application Firewall, and User Authentication. The 'User Authentication' menu is expanded to show 'Authentication Policy' and 'User Group'. The main area displays the configuration for an 'Authentication Policy' with the name 'kerberos'. The 'Host Status' is set to 'OFF'. The 'Type' is set to 'SAML'. The 'User Realm' field is empty with a placeholder text 'Required. Specify a realm.'. The 'Path' field contains a forward slash '/'. The 'User Group' dropdown menu is set to 'ker-218'.

The screenshot shows the configuration for a 'Virtual Server'. The 'Connection Limit' is set to '0'. The 'Interface' is set to 'port1'. Under the 'Resources' section, the 'Profile' is set to 'LB_PROF_HTTP', the 'Method' is set to 'LB_METHOD_ROUND_ROBIN', and the 'Clone Pool' is set to 'Click to select'. The 'Persistence' is set to 'Click to select'. The 'Real Server Pool' is set to 'server-pool1'. The 'Auth Policy' dropdown menu is set to 'kerberos'.



High Performance Network Security



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.