



FortiADC ADFS proxy Deployment Guide

Copyright© 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.

FortiADC ADFS proxy Deployment Guide

TABLE OF CONTENTS

1	About this Guide	4
2	AD FS Proxy scenario overview	4
2.1	Scenario1: Office365 in Pass Through Method.....	4
2.2	Scenario2: Exchange in Pass Through Method.....	5
2.3	Scenario3: Exchange in AD FS Method	5
3	AD FS Proxy Deployment configuration.....	6
3.1	Deploy AD FS Proxy for office365.....	6
3.1.1	use AD FS publish service to deploy.....	6
3.1.2	Configure office365 scenario using scripting.....	12
3.2	Deploy AD FS Proxy for Exchange in pass through mode	15
3.2.1	use AD FS publish service to deploy.....	15
3.2.2	Configure scripting and content routing	22
3.3	Deploy AD FS Proxy for Exchange in ADFS mode.....	26
3.3.1	use AD FS publish service to deploy.....	26
3.3.2	Configure using scripting	32
4	AD FS proxy Debug	37
4.1	Enable AD FS Proxy debug	37
4.2	Get AD FS proxy and publish status	37
5	AD FS Proxy Troubleshooting	37
5.1	Server Configuration Update Interval.....	37
5.2	AD FS Proxy configuration sync in ha environment.....	38

1 ABOUT THIS GUIDE

This guide details the steps required to configure the FortiADC AD FS Proxy function. The AD FS Proxy is a service that brokers a connection between external users and your internal AD FS server. It acts as a reverse proxy and typically resides in your organization's perimeter network (aka DMZ). As far as the user is concerned, they do not know they are talking to an AD FS proxy server, as the federation services are accessed by the same URLs.

This guide describes the configuration for AD FS Proxy authentication in each scenario, whether for Office365 or Exchange.

When the FortiADC works through AD FS Proxy, it is quite similar to how the WAP works. Both WAP and ADC support two preauthentication methods: besides AD FS, there is pass-through.

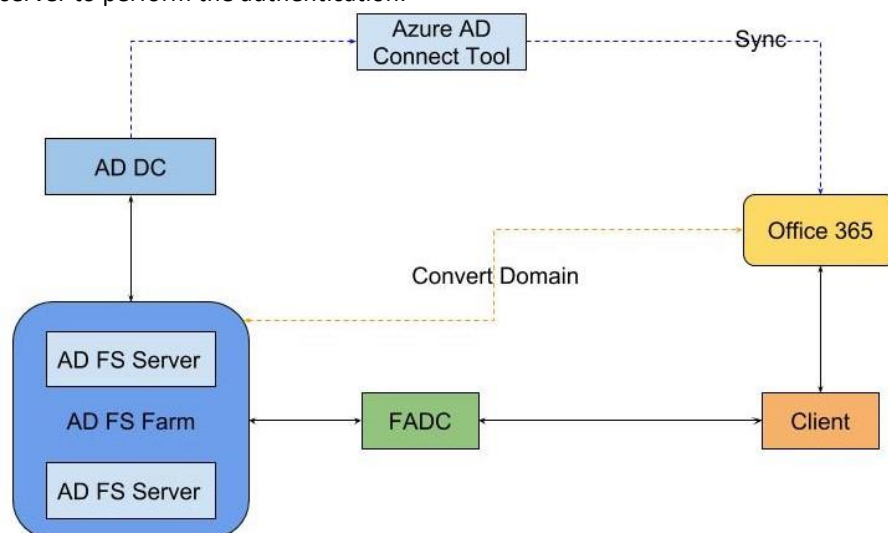
In the pass-through method, (1) no preauthentication is performed by AD FS Proxy, all requests are forwarded to the backend server. In AD FS(Active Directory Federation Services) method, (2) all unauthenticated client requests are redirected to the federation server. After successful authentication by AD FS, client requests are forwarded to the backend server.

Lastly, the FortiADC supports Office365 service in its pass-through method, since Office356 lies in the external web and the AD FS server in the internal web.

2 AD FS PROXY SCENARIO OVERVIEW

2.1 Scenario 1: Office365 in Pass Through Method

When the FortiADC devices are configured as AD FS proxy, FortiADC acts as the AD FS proxy between office365 and AD FS server. Client and office365 are both in the external web, while AD FS server is in the internal network. When client visits the office365 service, the request will be redirected to AD FS server to perform the authentication.



The chart above is the office365 in pass-through mode deployment. Normally, FortiADC receive the request from client to AD FS server, and load balances requests to the internal ADFS server.

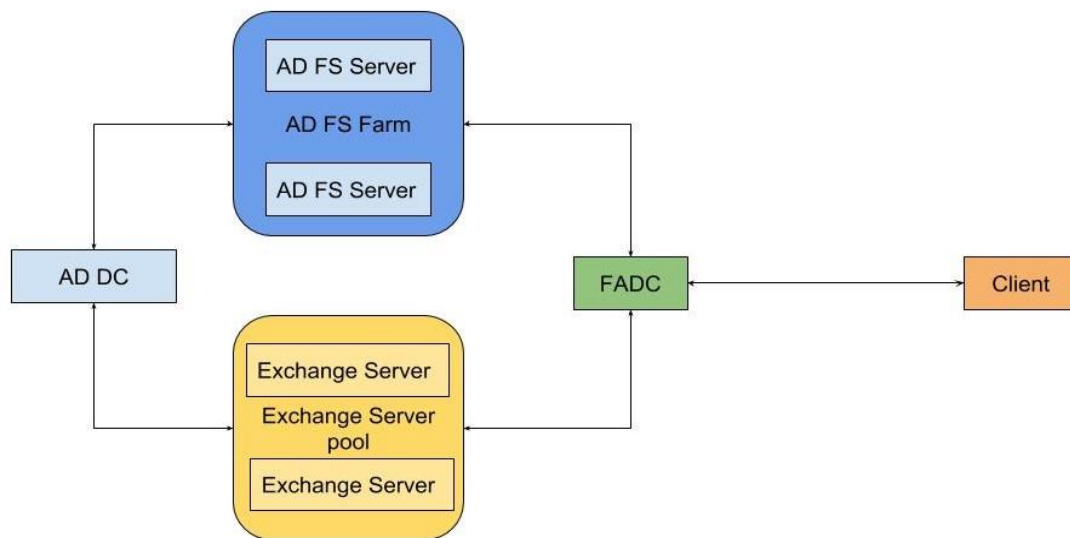
The following is the traffic flow for this scenario.

1. Client accesses the Office 365 cloud service;
2. Client is redirected to FADC, FADC delivers the request to an AD FS server in the AD FS Farm;
3. The AD FS server returns a web page and request username/password;
4. Client posts user name and password to AD FS Server;
5. After authentication, AD FS server sets cookie to client;
6. Client accesses AD FS server with cookie;

7. AD FS Server returns SAML token to client;
8. Client accesses office 365 with SAML token.

2.2 Scenario 2: Exchange in Pass Through Method

In this method, exchange server and AD FS server are both in the internal network, and when the client visits the exchange service, no preauthentication is performed by FortiADC; all requests are forwarded to the backend exchange server, and then the exchange server will redirect the request to the AD FS server.



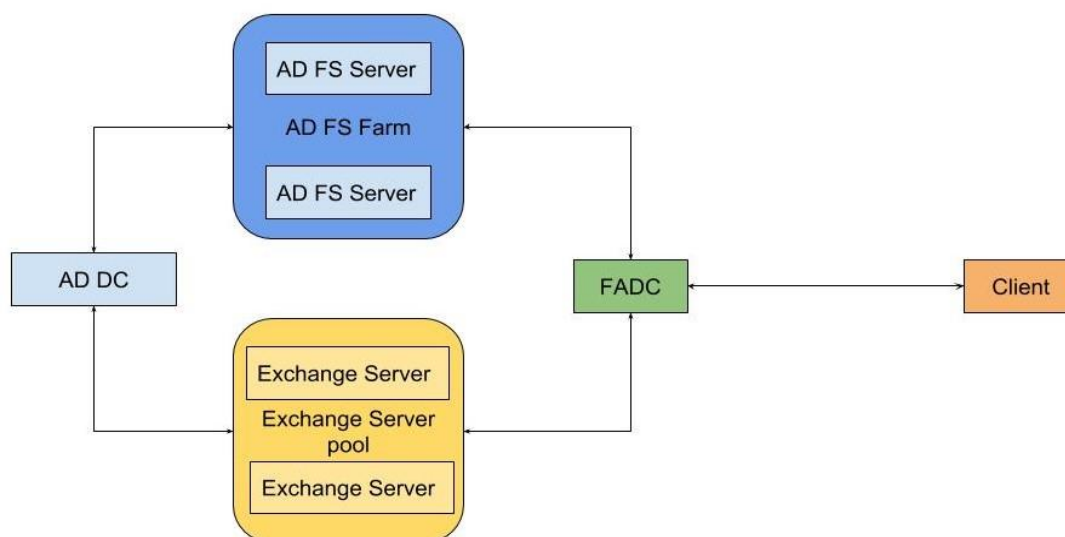
In this scenario, the traffic flow is same as the office365 scenario.

The following is the traffic flow for this scenario:

1. Client sends request to the exchange service (owa or ecp);
2. FADC forwards the request to the backend exchange server directly;
3. The exchange server receives the request and checks “not authenticated,” redirecting it to AD FS server;
4. Client requests that AD FS server perform the authentication. FADC delivers the request to an AD FS server in the AD FS Farm;
5. AD FS server returns a web page and request username/password;
6. Client posts user name and password to AD FS Server;
7. After authentication, the AD FS server sets cookie to client;
8. Client accesses AD FS server with cookie;
9. AD FS Server returns the SAML token to the client;
10. Client accesses exchange service with SAML token.

2.3 Scenario 3: Exchange in AD FS Method

In this method, exchange server and AD FS server are both in the internal network. All unauthenticated client requests are redirected to the federation server. After successful authentication by AD FS, client requests are forwarded to the backend exchange server.



The following is the traffic flow for this scenario.

1. Client sends request to FADC;
2. FADC redirects the request to AD FS Server;
3. AD FS Server sends response to client, and asks for the user name and password;
4. Client posts user name and password to AD FS Server;
5. After authentication, AD FS Server sets cookie to client;
6. AD FS Server redirects client's request to Exchange server with an authToken;
7. Client sends new GET request to Exchange server;
8. Exchange server sets cookie to client, and redirects client to AD FS Server;
9. AD FS Server returns SAML authentication message to client;
10. Client will POST SAML authentication message to Exchange Server;
11. After authentication, Exchange Server sets cookie to client;
12. Client accesses Exchange Server with cookie.

3 AD FS PROXY DEPLOYMENT CONFIGURATION

3.1 Deploy AD FS Proxy for office365

There are two methods to config AD FS Proxy for office365 scenario. The first method is to use AD FS publish service. The second is to use scripting and content routing. Here's how to configure the two methods.

3.1.1 Use AD FS publish service to deploy

1) It is recommended that the virtual server use AD FS publish service when office365 mode is deployed, because when the virtual server uses AD FS publish service, FortiADC will generate a script; in this script, some variables are set according to the AD FS publish service. The customer can also use the scripting and content routing to deploy office365 in chapter 3.1.2

Steps:

- (1) Add AD FS server pool

Pay attention:

```

S server uses https (443) to connect. The AD FS server pool must use the 443 port; in order to
make it work, it must set the real-server-ssl-profile. For real-server-ssl-profile, a local cert must
be used, and the ssl-sni-forward must be set.
config load-balance real-server-ssl-profile
edit "adfs1"
set ssl enable
set ssl-sni-forward enable
  
```

```

set local-cert Factory
next
end
config load-balance real-server
edit "adfs37"
set ip 10.0.58.37
next
end
config load-balance pool
edit "adfs37"
set real-server-ssl-profile adfs1
config pool_member
edit 1
set pool_member_service_port 443
set pool_member_cookie rs1
set real-server adfs37
next
end
next
end

```

Server SSL

Name

adfs1

SSL

ON

Customized SSL Ciphers Flag

OFF

SSL Cipher Suite List

☐ ECDHE-ECDSA-AES256-GCM-SHA384	☐ ECDHE-ECDSA-AES256-SHA384
☐ ECDHE-ECDSA-AES256-SHA	☐ ECDHE-ECDSA-AES128-GCM-SHA256
☐ ECDHE-ECDSA-AES128-SHA256	☐ ECDHE-ECDSA-AES128-SHA
☐ ECDHE-ECDSA-DES-CBC3-SHA	☐ ECDHE-ECDSA-RC4-SHA
☐ ECDHE-RSA-AES256-GCM-SHA384	☐ ECDHE-RSA-AES256-SHA384
☐ ECDHE-RSA-AES256-SHA	☒ DHE-RSA-AES256-GCM-SHA384
☒ DHE-RSA-AES256-SHA256	☒ DHE-RSA-AES256-SHA
☒ AES256-GCM-SHA384	☒ AES256-SHA256
☒ AES256-SHA	☐ ECDHE-RSA-AES128-GCM-SHA256
☐ ECDHE-RSA-AES128-SHA256	☐ ECDHE-RSA-AES128-SHA
☒ DHE-RSA-AES128-GCM-SHA256	☒ DHE-RSA-AES128-SHA256
☒ DHE-RSA-AES128-SHA	☒ AES128-GCM-SHA256
☒ AES128-SHA256	☒ AES128-SHA
☐ ECDHE-RSA-RC4-SHA	☒ RC4-SHA
☒ RC4-MD5	☐ ECDHE-RSA-DES-CBC3-SHA
☒ EDH-RSA-DES-CBC3-SHA	☒ DES-CBC3-SHA
☐ eNULL	

Allow SSL Versions

☒ sslv3
☒ tlsv1.0
☒ tlsv1.1
☒ tlsv1.2

Certificate Verify

Click to select

Local Certificate

Factory

SNI Forward Flag

ON

Save

Cancel

Real Server

Name

adfs37

Status

Enable

Disable

Maintain

Address

10.0.58.37

Address6

::

Real Server Pool

Name

adfs37

Address Type

IPv4

IPv6

Health Check

OFF

Real Server SSL Profile

adfs1

Member

Add Filter

Create New

ID	Name	Address	Health Check	Port
1	adfs37	10.0.58.37	inherited	443

Showing 1 to 1 of 1 entries

Show 10 entries

Previous 1 Next

(2) Add AD FS proxy

FortiADC adds an adfs-proxy for registering to AD FS server. The configuration should be set according to AD FS server; the fqdn is the same as AD FS federation service; the username should be the local administrator account on the AD FS server.

```
config user adfs-proxy
edit "o365"
set fqdn adfs.adfsfortiadc.com
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool adfs37
set username "adfs37\Administrator"
set password ENC skjgso1KvGVRmFh7RKUJkArz+X65udG2wAB8TajucCFOCbQe+zkNoH2eA+gL4Uv8yxNzoG2Iq/II4qGv4L/nLdQhtj26FsgdvsoxoWSvu8x+Al1
next
end
```

FortiADC-VM | VBRP (Working) | N/A | VS 2.1 VM Build 0425, 190

Search here

root

- Dashboard
- FortiView
- System
- Shared Resources
- Networking
- Server Load Balance
- Link Load Balance
- Global Load Balance
- Web Application Firewall
- User Authentication
 - Authentication Policy
 - User Group
 - Local User
 - Remote Server
 - Authentication Relay
 - SAML
 - AD FS Proxy

AD FS Proxy

Name	Federation Service Name	Status	Availability	AD FS Server Pool
adfs37	adfs.adfsfortiadc.com	Enable	✓	adfs37

Showing 1 to 1 of 1 entries | Show 10 entries

Proxy

Name: adfs37

Status:

Method:

AD FS Server Pool: adfs37

Federation Service Name: adfs.adfsfortiadc.com

User Name: adfs37\Administrator

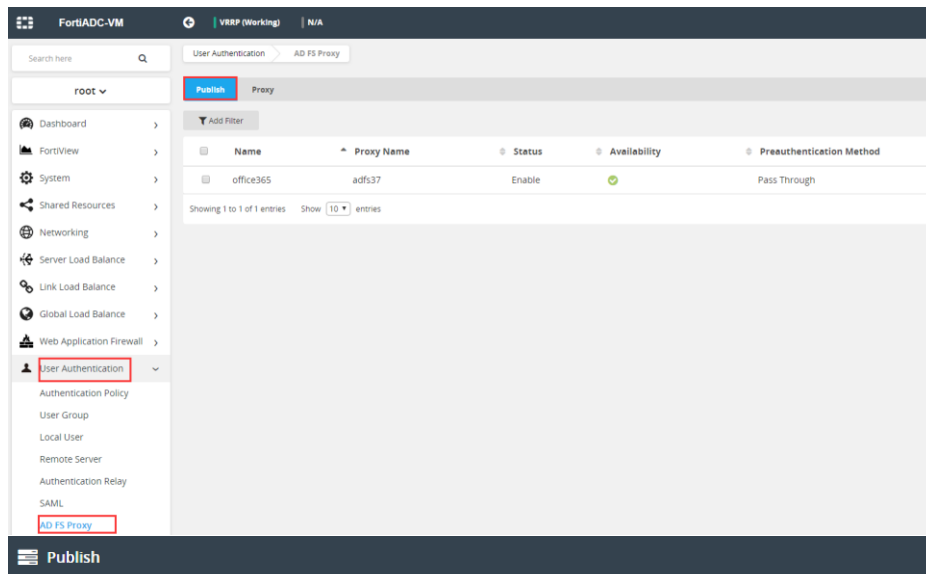
Password:

Server Configuration Update Interval: _____

(3) Add AD FS publish

In office365 scenario, the method uses pass-through. The external-url should be same as it is in AD FS server.

```
config user adfs-publish
edit "o365"
set adfs-proxy o365
set external-url https://adfs.adfsfortiadc.com/adfs/
next
end
```



Name
office365

Status

AD FS Proxy
adfs37

Preauthentication Method

External URL

Example: https://certauth.o365.com/owa/

- (4) Set AD FS publish service to virtual server
As AD FS server uses the https(443) connection, the office365 virtual server must configure LB_PROF_HTTPS profile and the port must use 443.

```
config load-balance virtual-server
edit "o365"
set type l7-load-balance
set interface port1
set ip 10.0.58.39
set port 443
set load-balance-profile LB_PROF_HTTPS
set client-ssl-profile LB_CLIENT_SSL_PROF_DEFAULT
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool adfs37
set traffic-group default
set adfs-published-service office365
next
end
```

Virtual Server

Basic **General** Security SSL Traffic Mirror Application Optimization Monitoring

Configuration

Address: 10.0.58.39
Example: 192.0.2.1

Port: 443
Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit: 0
Default: 0 Range: 0-100000000 concurrent connections

Interface: port1

Public IP Type: IPv4 IPv6

Public IPv4: 0.0.0.0
Example: 192.0.2.1

Resources

Profile: LB_PROF_HTTPS

Client SSL Profile: LB_CLIENT_SSL_PROF_DEFAULT

Persistence: Click to select

Method: LB_METHOD_ROUND_ROBIN

Real Server Pool: adfs37

Clone Pool: Click to select

Auth Policy: Click to select

Scripting: OFF
To use scripts to manipulate compressed HTTP/HTTPS data body, you must have decompression rules configured first.

AD FS Published Service: office365

Save Cancel

2) Configure adfs proxy advance option

As AD FS proxy will register to AD FS server, in the register connection, customer can configure some timeout to adapt to the AD FS server.

In “User Authentication->AD FS Proxy->Proxy” page:

FortiADC-VM vROP (Working) N/A VS 2.1 VM Build0425,190

Search here

User Authentication > AD FS Proxy

Publish Proxy

Add Filter

Name	Federation Service Name	Status	Availability	AD FS Server Pool
adfs37	adfs.adfsfortadc.com	Enable	OK	adfs37

Showing 1 to 1 of 1 entries Show 10 entries

Dashboard FortView System Shared Resources Networking Server Load Balance Link Load Balance Global Load Balance Web Application Firewall **User Authentication** AD FS Proxy

Open the proxy and configure the timeout as customer needed:

Proxy

adfs3/Administrator

Password

Server Configuration Update Interval

300

Default: 300 Range: 1-8640000

Register Timeout

12

Default: 12 Range: 1-3600

Connect Timeout

5

Default: 5 Range: 1-3600

Response Timeout

6

Default: 6 Range: 1-3600

Keepalive Timeout

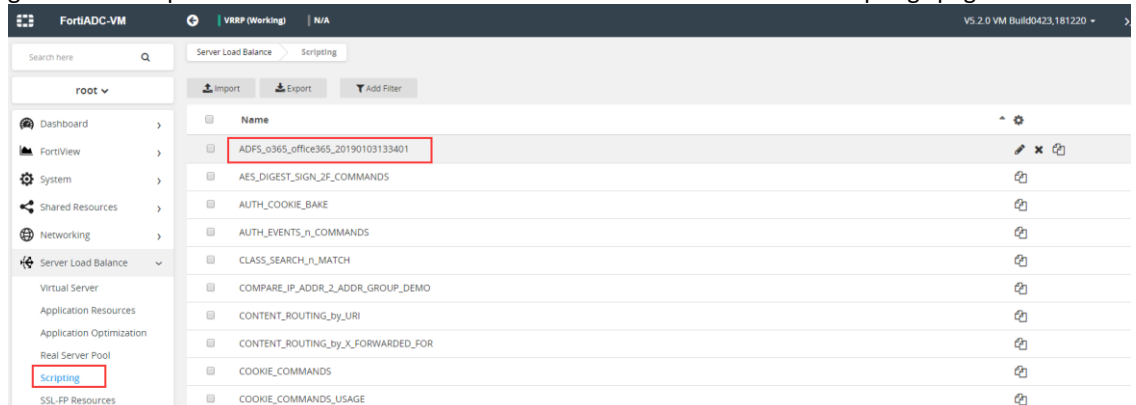
300

Default: 300 Range: 1-3600

Save Cancel

3.1.2 Configure office365 scenario using scripting

As configuration in 3.1.1, when the virtual server uses the AD FS publish service, FortiADC will generate a script at the same time. You can see it in “Server Load Balance->Scripting” page:



The script is named ADFS_VIRTUAL_SERVERNAME_PUBLISHNAME_timestamp. This script defines the action that office365 scenario requires. When the virtual server unsets AD FS publish service, FortiADC will delete this script at the same time.

Scripting

Name

ADFS_o365_office365_20190103133401

```

1 when RULE_INIT{
2     --should be replaced according to the publish settings
3     pub_uri = "/adfs/"
4     external_host = "adfs.adfsfortiadc.com"
5 }
6
7 when HTTP_REQUEST{
8     uri = HTTP:uri_get()
9     host = HTTP:header_get_value("Host")
10    path = HTTP:path_get()
11
12    if host:find(external_host) and uri:starts_with(pub_uri) then
13        --insert ADFS header
14        --HTTP:header_insert(header_name, value)
15        cip = IP:client_addr() -- get client ip address
16        HTTP:header_insert("X-MS-Endpoint-Absolute-Path", path)
17        HTTP:header_insert("X-MS-Forwarded-Client-IP", cip)
18        HTTP:header_insert("X-MS-Proxy", "FortiADC")
19    else
20        HTTP:close()
21        debug("no matches domain for host: %s and uri %s\n", host, uri)
22    end
23 }

```

Save

Cancel

Customer can use scripting instead of AD FS publish service.

Steps:

- (1) Copy this script.

Search here

Q

Server Load Balance

Scripting

root

Dashboard

FortiView

System

Shared Resources

Networking

Server Load Balance

Virtual Server

Application Resources

Application Optimization

Real Server Pool

Scripting

SSL-FP Resources

Import

Export

Add Filter

Name
ADFS_O365
ADFS_o365_office365_20190103133401
AES_DIGEST_SIGN_2F_COMMANDS
AUTH_COOKIE_BAKE
AUTH_EVENTS_n_COMMANDS
CLASS_SEARCH_n_MATCH
COMPARE_IP_ADDR_2_ADDR_GROUP_DEMO
CONTENT_ROUTING_by_URI
CONTENT_ROUTING_by_X_FORWARDED_FOR
COOKIE_COMMANDS

- (2) In virtual server, unset AD FS publish service

```

config load-balance virtual-server
edit "o365"
    unset adfs-published-service
next
end

```

Virtual Server

Public IP Type

IPv4 IPv6

Public IPv4

0.0.0.0

Example: 192.0.2.1

Resources

Profile

LB_PROF_HTTPS

Persistence

Click to select.

Real Server Pool

adfs37

Auth Policy

Click to select

AD FS Published Service

Click to select

Client SSL Profile

LB_CLIENT_SSL_PROF_DEFAULT

Method

LB_METHOD_ROUND_ROBIN

Clone Pool

Click to select

Scripting

OFF

To use scripts to manipulate compressed HTTP/HTTPS data body, you must have decompression rules configured first.

Save

Cancel

(3) Set script copied in (1) to virtual server

```

config load-balance virtual-server
edit "o365"
set type l7-load-balance
set interface port1
set ip 10.0.58.39
set port 443
set load-balance-profile LB_PROF_HTTPS
set client-ssl-profile LB_CLIENT_SSL_PROF_DEFAULT
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool adfs37
set scripting-flag enable
set scripting-list ADFS_o365
set traffic-group default
next
end
  
```

Virtual Server

LB_PROF_HTTPS

LB_CLIENT_SSL_PROF_DEFAULT

Persistence

Click to select.

Method

LB_METHOD_ROUND_ROBIN

Real Server Pool

adfs37

Clone Pool

Click to select

Auth Policy

Click to select

Scripting

ON

To use scripts to manipulate compressed HTTP/HTTPS data body, you must have decompression rules configured first.

AD FS Published Service

Click to select

Scripting List

Selected Items

ADFS_o365

Available Items

Create New

HTTP_2_HTTPS_REDIRECT

HTTP_2_HTTPS_REDIRECT_FULL_URL

Double-click to deselect. Drag to reorder.

Save

Cancel

Note:

- (1) When configure AD FS publish service to virtual server, FortiADC generates a script. This script will be deleted by FortiADC when virtual server unsets AD FS publish service.

- (2) As AD FS publish uses the adfs federation service, the client should configure the mapping between adfs federation service and virtual server ip address, such as:
 adfs.adfsfortiadc.com 10.0.58.39 (10.0.58.39 is virtual server ip)
 When client requests office365 service, like <https://portal.microsoft.com>, the request will be redirected to FADC(10.0.58.39) to perform authentication.
- (3) AD FS publish cannot configure disabled AD FS proxy
- (4) Virtual server cannot configure disabled AD FS publish

3.2 Deploy AD FS Proxy for Exchange in pass through mode

In this scenario, as the AD FS server and exchange server are both in the internal network, FortiADC should add two pools for AD FS server and exchange server.

3.2.1 use AD FS publish service to deploy

1) config Steps:

- (1) Add AD FS server pool

Pay attention:

As AD FS server uses https(443) to connect, the AD FS server pool must use 443 port and set real-server-ssl-profile. In real-server-ssl-profile, a local cert must be used, and the ssl-sni-forward must be set.

```
config load-balance real-server-ssl-profile
edit "adfs"
set ssl enable
set ssl-sni-forward enable
set local-cert Factory
next
end
config load-balance real-server
edit "adfs103"
set ip 10.58.0.103
next
end
config load-balance pool
edit "adfs103"
set real-server-ssl-profile adfs
config pool_member
edit 1
set pool_member_service_port 443
set pool_member_cookie rs1
set real-server adfs103
next
end
next
end
```

Server SSL

Name

adfs

SSL

ON

Customized SSL Ciphers Flag

OFF

SSL Cipher Suite List

☐ ECDHE-ECDSA-AES256-GCM-SHA384
☐ ECDHE-ECDSA-AES256-SHA
☐ ECDHE-ECDSA-AES128-SHA256
☐ ECDHE-ECDSA-DES-CBC3-SHA
☐ ECDHE-RSA-AES256-GCM-SHA384
☐ ECDHE-RSA-AES256-SHA
☐ DHE-RSA-AES256-SHA256
☒ AES256-GCM-SHA384
☒ AES256-SHA
☐ ECDHE-RSA-AES128-SHA256
☐ DHE-RSA-AES128-GCM-SHA256
☐ DHE-RSA-AES128-SHA
☒ AES128-SHA256
☐ ECDHE-RSA-RC4-SHA
☒ RC4-MD5
☐ EDH-RSA-DES-CBC3-SHA
☐ eNULL

☐ ECDHE-ECDSA-AES256-SHA384
☐ ECDHE-ECDSA-AES128-GCM-SHA256
☐ ECDHE-ECDSA-AES128-SHA
☐ ECDHE-ECDSA-RC4-SHA
☒ ECDHE-RSA-AES256-SHA384
☒ DHE-RSA-AES256-GCM-SHA384
☒ DHE-RSA-AES256-SHA
☒ AES256-SHA256
☐ ECDHE-RSA-AES128-GCM-SHA256
☐ ECDHE-RSA-AES128-SHA
☐ DHE-RSA-AES128-SHA256
☒ AES128-GCM-SHA256
☒ AES128-SHA
☒ RC4-SHA
☐ ECDHE-RSA-DES-CBC3-SHA
☐ DES-CBC3-SHA

Allow SSL Versions

☒ sslv3
☒ tlsv1.0
☒ tlsv1.1
☒ tlsv1.2

Certificate Verify

Click to select

Local Certificate

Factory

SNI Forward Flag

ON

Save

Cancel

Real Server

Name

adfs103

Status

Enable

Disable

Maintain

Address

10.58.0.103

Address6

::

Real Server Pool

Name

adfs103

Address Type

IPv4 IPv6

Health Check

OFF

Real Server SSL Profile

adfs

Member

Add Filter

Create New

ID	Name	Address	Health Check	Port	
1	adfs103	10.58.0.103	inherited	443	

Showing 1 to 1 of 1 entries

Show 10 entries

Previous 1 Next

(2) Add AD FS proxy

FortiADC adds an adfs-proxy for registering to AD FS server. So, the configuration should be set according to AD FS server; the fqdn is the same as it is for AD FS federation service; the username should be the local administrator account on the AD FS server.

config user adfs-proxy

edit "register_58_110"

set fqdn adfs.adfsfortiadc.com

set load-balance-method LB_METHOD_ROUND_ROBIN

set load-balance-pool adfs103

set username "adfs103\Administrator"

set password ENC

skjgso1KvGVRmFh7RKUJkArz+X65udG2wAB8TajucFCObQe+zkNoH2eA+gL4Uv8yxNzZoG2lq/ll4qGv4L/nLdQhtj26FsgdvsoxoWSvu8x+Al1

next

end

Search here

User Authentication > AD FS Proxy

vd1

Dashboard

FortiView

System

Shared Resources

Networking

Server Load Balance

Link Load Balance

Global Load Balance

Web Application Firewall

User Authentication

Authentication Policy

User Group

Local User

Remote Server

Authentication Relay

SAML

AD FS Proxy

Publish

Proxy

Add Filter

Name	Federation Service Name	Status	Availability	AD FS Server Pool
register_58_110	adfs.adfsfortiadc.com	Enable		adfs103

Showing 1 to 1 of 1 entries

Show 10 entries

Proxy

Name

Status

Method

AD FS Server Pool

Federation Service Name

User Name

Password

Server Configuration Update Interval

(3) Add AD FS publish

In this scenario, the method uses pass-through.

```

config user adfs-publish
edit "passthrough-owa"
set status enable
set adfs-proxy register_58_110
set pre-auth Pass-through
set external-url https://mail.adfsfortiadc.com/owa/
next
end
    
```

Search here

vd1

Dashboard
FortiView
System
Shared Resources
Networking
Server Load Balance
Link Load Balance
Global Load Balance
Web Application Firewall
User Authentication
Authentication Policy
User Group
Local User
Remote Server
Authentication Relay
SAML
AD FS Proxy

User Authentication > AD FS Proxy

Publication

Proxy

Add Filter

Name	Proxy Name	Status	Availability	Preauthentication Method
passthrough-ecp	register_58_110	Enable	✓	Pass Through
passthrough-owa	register_58_110	Enable	✓	Pass Through
publish-ecp	register_58_110	Enable	✓	ADFS
publish-owa	register_58_110	Enable	✓	ADFS
xxxxxxx	register_58_110	Disable	✗	ADFS

Showing 1 to 5 of 5 entries Show 10 entries

 Publish

Name

passthrough-owa

Status

Disable

Enable

AD FS Proxy

register_58_110

Preauthentication Method

Pass Through

ADFS

External URL

https://mail.adfsfortiadc.com/owa/

Example: https://certauth.0365.com/owa/

(4) Add exchange server pool

```
config load-balance real-server
edit "exchange102"
set ip 10.58.0.102
next
end
config load-balance pool
edit "exchange102"
set real-server-ssl-profile adfs
config pool_member
edit 1
set pool_member_service_port 443
set pool_member_cookie rs1
set real-server exchange102
next
end
next
```

 Real Server

Name

exchange102

Status

Enable

Disable

Maintain

Address

10.58.0.102

Address6

::

Real Server Pool

Name

exchange102

Address Type

IPv4 IPv6

Health Check

OFF

Real Server SSL Profile

adfs

Member

Add Filter

Create New

ID	Name	Address	Health Check	Port	
1	exchange102	10.58.0.102	inherited	443	

Showing 1 to 1 of 1 entries

Show 10 entries

Previous 1 Next

- (5) Add virtual server, set AD FS publish service to virtual server

```

endconfig load-balance virtual-server
edit "passthrough_owa"
set type l7-load-balance
set interface port2
set ip 10.58.1.102
set port 443
set load-balance-profile LB_PROF_HTTPS
set client-ssl-profile LB_CLIENT_SSL_PROF_DEFAULT
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool exchange102
set traffic-group default
set adfs-published-service passthrough-owa
next
end

```

Virtual Server

Basic

General

Security

SSL Traffic Mirror

Application Optimization

Monitoring

Configuration

Address

10.58.1.102

Example: 192.0.2.1

Port

443

Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit

0

Default: 0 Range: 0-100000000 concurrent connections

Interface

port2

Public IP Type

IPv4

IPv6

Public IPv4

0.0.0.0

Example: 192.0.2.1

Resources

Profile

LB_PROF_HTTPS

Client SSL Profile

LB_CLIENT_SSL_PROF_DEFAULT

Persistence

Click to select.

Method

LB_METHOD_ROUND_ROBIN

Real Server Pool

exchange102

Clone Pool

Click to select

Auth Policy

Click to select

Scripting

OFF

To use scripts to manipulate compressed HTTP/HTTPS data body, you must have decompression rules configured first.

AD FS Published Service

passthrough-owa

Save

Cancel

2) Configure adfs proxy advance option

AD FS proxy will register to the AD FS server. In the register connection, the customer can configure the timeouts to adapt to the AD FS server.

In “User Authentication->AD FS Proxy->Proxy” page:

FortiADC-VM

VRRP (Working)

N/A

V5.2.0 VM Build0423.181220

Search here

Q

vd1

Dashboard

FortiView

System

Shared Resources

Networking

Server Load Balance

Link Load Balance

Global Load Balance

Web Application Firewall

User Authentication

Authentication Policy

User Group

Local User

Remote Server

Authentication Relay

SAML

AD FS Proxy

User Authentication

AD FS Proxy

Publish

Proxy

Add Filter

Name	Federation Service Name	Status	Availability	AD FS Server Pool
register_58_110	adfs.adfsfortiadc.com	Enable	🟢	adfs103

Showing 1 to 1 of 1 entries Show 10 entries

Open the proxy and configure the timeout as customer needed:

Proxy

Username: adfs103\Administrator

Password:

Server Configuration Update Interval: 300
Default: 300 Range: 1-8640000

Register Timeout: 12
Default: 12 Range: 1-3600

Connect Timeout: 5
Default: 5 Range: 1-3600

Response Timeout: 6
Default: 6 Range: 1-3600

Keepalive Timeout: 300
Default: 300 Range: 1-3600

Save Cancel

3.2.2 Configure scripting and content routing

As shown in 3.2.1, when configuring AD FS publish service to the virtual server, a script is generated automatically. Customer can use scripting instead of AD FS publish service.

In “Server Load Balance->Scripting” page:

FortiADC-VM | VRMP (Working) | N/A | VS 2.0 VM Build0423,181220

Search here

Server Load Balance > Scripting

Import Export Add Filter

Name	
adfs_passthrough_ecp	
adfs_passthrough_owa	
ADFS_passthrough_owa_passthrough-owa_20190103131208	
adfs_publish_ecp	
adfs_publish_owa	
AES_DIGEST_SIGN_2F_COMMANDS	
AUTH_COOKIE_BAKE	
AUTH_EVENTS_n_COMMANDS	
CLASS_SEARCH_n_MATCH	
COMPARE_IP_ADDR_2_ADDR_GROUP_DEMO	

Left sidebar: Dashboard, FortiView, System, Shared Resources, Networking, Server Load Balance (Virtual Server, Application Resources, Application Optimization, Real Server Pool, **Scripting**, SSL-FP Resources)

Opening this script, you can get the action that FortiADC will then operate. In this script, FortiADC will forward requests to different backend server pools, by using content routing. So the customer should add content routings that as the same as those used in scripting.

Scripting

Name

ADFS_passthrough_owa_passthrough-owa_20190103131208

```

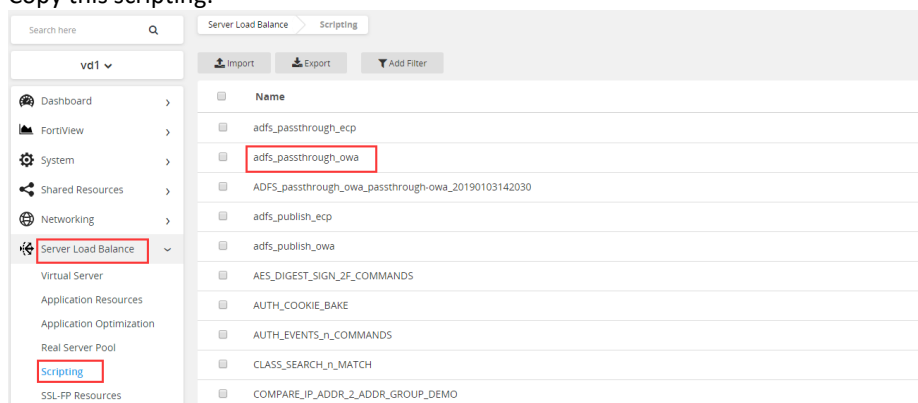
1  when RULE_INIT{
2      pub_uri = "/owa/"
3      external_host = "mail.adfsfortiadc.com"
4      adfs_server_domain = "adfs.adfsfortiadc.com"
5  }
6
7  when HTTP_REQUEST{
8      uri = HTTP:uri_get()
9      host = HTTP:header_get_value("Host")
10     path = HTTP:path_get()
11
12     --content-routing
13     --"msapp" "adfsserver" should have created in content-routing module
14     if host:find(external_host) and uri:starts_with(pub_uri) then
15         LB:routing("exchange102")
16     elseif host:find(adfs_server_domain) then
17         LB:routing("adfs_103")
18     else
19         debug("no matches domain for host: %s and uri %s\n", host, uri)
20         HTTP:close()
21     end
22 }

```

Customer can use scripting and content routing instead of AD FS publish service.

Steps:

- (1) Copy this scripting.



- (2) In virtual server, unset AD FS publish service

```

config load-balance virtual-server
edit "passthrough_owa"
unset adfs-published-service
next
end

```

- (3) Add content routing

It is the same as that used in the scripting, like in the previous example, content routing "exchange102" using real-server-pool "exchange102", and content routing "adfs103" using real-server-pool "adfs103"

```

config load-balance content-routing
edit "exchange102"
set load-balance-pool exchange102
config match-condition
end
next
edit "adfs103"
set load-balance-pool adfs103
config match-condition
end
next
end

```

Name	Type	Real Server	Match Condition Count
adfs103	Layer 7	adfs103	0
adfs_all	Layer 7	adfs_all	0
exchange102	Layer 7	exchange102	0

Content Routing

Name: adfs103

Type: Layer 4 Layer 7

General

Schedule Pool: OFF

Real Server Pool: adfs103

Persistence: Click to select Inherit

Method: Inherit

Content Routing

Name: exchange102

Type: Layer 4 Layer 7

General

Schedule Pool: OFF

Real Server Pool: exchange102

Persistence: Click to select Inherit

Method: Inherit

(4) For scripting copied in step 1 and content routing in step 3, set them to the virtual server.

```
config load-balance virtual-server
edit "passthrough_owa"
set type l7-load-balance
set interface port2
set ip 10.58.1.102
set port 443
set load-balance-profile LB_PROF_HTTPS
set client-ssl-profile LB_CLIENT_SSL_PROF_DEFAULT
set content-routing enable
set content-routing-list adfs103 exchange102
set load-balance-method LB_METHOD_ROUND_ROBIN
set scripting-flag enable
```

```
set scripting-list ADFS_passthrough_owa
set traffic-group default
next
end
```

Virtual Server

Basic General Security SSL Traffic Mirror Application Optimization Monitoring

Name
passthrough_owa

Type
Layer 7 Layer 4 Layer 2

Status
Disable Enable Maintain

Address Type
IPv4 IPv6

Traffic Group
default

Specifics

Content Routing
ON

Content Routing List

Selected Items
adfs103
exchange102

Available Items
Create New
adfs_all

Double-click to deselect. Drag to reorder.

Double-click to select.

Virtual Server

Basic **General** Security SSL Traffic Mirror Application Optimization Monitoring

Configuration

Address
10.58.1.102
Example: 192.0.2.1

Port
443
Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit
0
Default: 0 Range: 0-100000000 concurrent connections

Interface
port2

Public IP Type
IPv4 IPv6

Public IPv4
0.0.0.0
Example: 192.0.2.1

Resources

Profile
LB_PROF_HTTPS

Client SSL Profile
LB_CLIENT_SSL_PROF_DEFAULT

Persistence
Click to select.

Method
LB_METHOD_ROUND_ROBIN

Clone Pool
Click to select.

Auth Policy
Click to select.

Scripting
ON

To use scripts to manipulate compressed HTTP/HTTPS data body, you must have decompression rules configured first.

Scripting List

Selected Items
adfs_passthrough_owa

Available Items
Create New
HTTP_2_HTTPS_REDIRECT
HTTP_2_HTTPS_REDIRECT_FULL_URL

Double-click to deselect. Drag to reorder.

Double-click to select.

Note:

- (1) Upon configuring AD FS publish service to virtual server, FortiADC generates a script. This script will be deleted by FortiADC when virtual server unsets AD FS publish service.

- (2) Since AD FS publish uses adfs federation service, the client should configure the mapping between adfs federation service and VIRTUAL SERVER ip address, such as:
 adfs.adfsfortiadc.com 10.58.1.102(virtual server ip)
 mail.adfsfortiadc.com 10.58.1.102
 Then client requests exchange service: https://mail.adfsfortiadc.com/owa/
- (3) AD FS publish cannot configure disabled AD FS proxy
- (4) Virtual server cannot configure disabled AD FS publish

3.3 Deploy AD FS Proxy for Exchange in ADFS mode

3.3.1 use AD FS publish service to deploy

It is recommended that the virtual server use AD FS publish service when exchange mode is deployed. When virtual server uses AD FS publish service, FortiADC will generate a script; in this script, some variables are set according to the AD FS publish service. The customer can also use scripting and content routing to deploy exchange-ADFS.

Steps:

- (1) Add AD FS server pool

Since the AD FS server uses https(443) to connect, the AD FS server pool must use 443 port and set real-server-ssl-profile. In real-server-ssl-profile, a local cert must be used, and the ssl-sni-forward must be set.

```
config load-balance real-server-ssl-profile
edit "adfs"
set ssl enable
set ssl-sni-forward enable
set local-cert Factory
next
end
config load-balance real-server
edit "adfs103"
set ip 10.58.0.103
next
end
config load-balance pool
edit "adfs103"
set real-server-ssl-profile adfs
config pool_member
edit 1
set pool_member_service_port 443
set pool_member_cookie rs1
set real-server adfs103
next
end
next
end
```

Server SSL

Name

adfs

SSL

ON

Customized SSL Ciphers Flag

OFF

SSL Cipher Suite List

☐ ECDHE-ECDSA-AES256-GCM-SHA384
☐ ECDHE-ECDSA-AES256-SHA
☐ ECDHE-ECDSA-AES128-SHA256
☐ ECDHE-ECDSA-DES-CBC3-SHA
☐ ECDHE-RSA-AES256-GCM-SHA384
☐ ECDHE-RSA-AES256-SHA
☐ DHE-RSA-AES256-SHA256
☒ AES256-GCM-SHA384
☒ AES256-SHA
☐ ECDHE-RSA-AES128-SHA256
☐ DHE-RSA-AES128-GCM-SHA256
☐ DHE-RSA-AES128-SHA
☒ AES128-SHA256
☐ ECDHE-RSA-RC4-SHA
☒ RC4-MD5
☐ EDH-RSA-DES-CBC3-SHA
☐ eNULL

☐ ECDHE-ECDSA-AES256-SHA384
☐ ECDHE-ECDSA-AES128-GCM-SHA256
☐ ECDHE-ECDSA-AES128-SHA
☐ ECDHE-ECDSA-RC4-SHA
☒ ECDHE-RSA-AES256-SHA384
☒ DHE-RSA-AES256-GCM-SHA384
☒ DHE-RSA-AES256-SHA
☒ AES256-SHA256
☐ ECDHE-RSA-AES128-GCM-SHA256
☐ ECDHE-RSA-AES128-SHA
☐ DHE-RSA-AES128-SHA256
☒ AES128-GCM-SHA256
☒ AES128-SHA
☒ RC4-SHA
☐ ECDHE-RSA-DES-CBC3-SHA
☐ DES-CBC3-SHA

Allow SSL Versions

☒ sslv3
☒ tlsv1.0
☒ tlsv1.1
☒ tlsv1.2

Certificate Verify

Click to select

Local Certificate

Factory

SNI Forward Flag

ON

Save

Cancel

Real Server

Name

adfs103

Status

Enable

Disable

Maintain

Address

10.58.0.103

Address6

::

Real Server Pool

Name

adfs103

Address Type

IPv4 IPv6

Health Check

OFF

Real Server SSL Profile

adfs

Member

Add Filter

Create New

ID	Name	Address	Health Check	Port	
1	adfs103	10.58.0.103	inherited	443	

Showing 1 to 1 of 1 entries

Show 10 entries

Previous 1 Next

(2) Add AD FS proxy

FortiADC add an adfs-proxy for registering to AD FS server. So, the configuration should set according to AD FS server, the fqdn same as AD FS federation service, username should can login to the AD FS service.

```
config user adfs-proxy
edit "register_58_110"
set fqdn adfs.adfsfortiadc.com
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool adfs103
set username "adfs103\Administrator"
set password ENC skjgso1KvGVRmFh7RKUJkArz+X65udG2wAB8TajucFCObQe+zkNoH2eA+gL4Uv8yxNzZoG2Iq/ll4qGv4L/nLdQhtj26FsgdvSxoWSvu8x+Al1
next
end
```

Search here

vd1

Dashboard

FortiView

System

Shared Resources

Networking

Server Load Balance

Link Load Balance

Global Load Balance

Web Application Firewall

User Authentication

Authentication Policy

User Group

Local User

Remote Server

Authentication Relay

SAML

AD FS Proxy

User Authentication > AD FS Proxy

Publish

Proxy

Add Filter

Name	Federation Service Name	Status	Availability	AD FS Server Pool
register_58_110	adfs.adfsfortiadc.com	Enable	✓	adfs103

Showing 1 to 1 of 1 entries

Show 10 entries

Proxy

Name

register_58_110

Status

Disable Enable

Method

None LB METHOD ROUND ROBIN

AD FS Server Pool

adfs103

Federation Service Name

adfs.adfsfortiadc.com

User Name

adfs103\Administrator

Password

Server Configuration Update Interval

Save Cancel

- (3) After the AD FS proxy registers successfully in AD FS server, FortiADC will get all the relyingpartytrust from AD FS server. For example, in my test environment, the relypartytrust is Device Registration Service, ExchangeOWA, ExchangeECP. Then FortiADC will save them as shown below, and in FADC, relyparttrust should not be edited, as they are required from AD FS server after AD FS Proxy in FADC registers successfully.

```
config user adfs-relying-party
edit "register_58_110-Device_Registration_Service-1545054427"
set proxy register_58_110
set relying-party-trust "Device Registration Service"
next
edit "register_58_110-ExchangeOWA-1545054427"
set proxy register_58_110
set relying-party-trust ExchangeOWA
next
edit "register_58_110-ExchangeECP-1545054427"
set proxy register_58_110
set relying-party-trust ExchangeECP
next
end
```

- (4) Add AD FS publish

In this scenario, the method uses ADFS. The backend-server-url should be same as in AD FS server. The external-url is the url that client will visit.

That is to say, in my example, customer request exchange service via:
https://100.adfsfortiadc.com/owa/

```
config user adfs-publish
edit "publish-owa"
set adfs-proxy register_58_110
set pre-auth ADFS
set relying-party register_58_110-ExchangeOWA-1545054427
set external-url https://100.adfsfortiadc.com/owa/
set backend-server-url https://mail.adfsfortiadc.com/owa/
```

next
end

Search here

vd1

- Dashboard
- FortView
- System
- Shared Resources
- Networking
- Server Load Balance
- Link Load Balance
- Global Load Balance
- Web Application Firewall
- User Authentication

User Authentication > AD FS Proxy

AD FS Proxy

Name	Proxy Name	Status	Availability	Preauthentication Method
passthrough-ecp	register_58_110	Enable	✓	Pass Through
passthrough-owa	register_58_110	Enable	✓	Pass Through
publish-ecp	register_58_110	Enable	✓	ADFS
publish-owa	register_58_110	Enable	✓	ADFS
xxxxxxx	register_58_110	Disable	✗	ADFS

Showing 1 to 5 of 5 entries

Publish

Name
publish-owa

Status

AD FS Proxy
register_58_110

Preauthentication Method

Relying Party
register_58_110-ExchangeOWA-1545054427

External URL

Example: https://certauth.o365.com/owa/

Backend Server URL

Example: https://certauth.o365.com/owa/

- (5) Add exchange server pool and virtual server, set AD FS publish service to virtual server.

```

config load-balance virtual-server
edit "publish_owa"
set type l7-load-balance
set interface port2
set ip 10.58.1.100
set port 443
set load-balance-profile LB_PROF_HTTPS
set client-ssl-profile LB_CLIENT_SSL_PROF_DEFAULT
set load-balance-method LB_METHOD_ROUND_ROBIN
set load-balance-pool exchange102
set traffic-group default
set adfs-published-service publish-owa
next
end

```

Virtual Server

Basic **General** Security SSL Traffic Mirror Application Optimization Monitoring

Configuration

Address: 10.58.1.100
Example: 192.0.2.1

Port: 443
Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit: 0
Default: 0 Range: 0-100000000 concurrent connections

Interface: port2

Public IP Type: **IPv4** IPv6

Public IPv4: 0.0.0.0
Example: 192.0.2.1

Resources

Profile: LB_PROF_HTTPS

Client SSL Profile: LB_CLIENT_SSL_PROF_DEFAULT

Persistence: Click to select

Method: LB_METHOD_ROUND_ROBIN

Real Server Pool: exchange102

Clone Pool: Click to select

Auth Policy: Click to select

Scripting: OFF
To use scripts to manipulate compressed HTTP/HTTPS data body, you must have decompression rules configured first.

AD FS Published Service: publish-owa

Save Cancel

2) Configure adfs proxy advance option

AD FS proxy will register to AD FS server, and in the register connection, the customer can configure some timeouts to adapt to the AD FS server.

In "User Authentication->AD FS Proxy->Proxy" page:

FortiADC-VM VRRP (Working) N/A VS 2.0 VM Build0423,181220

Search here

vd1

Dashboard FortiView System Shared Resources Networking Server Load Balance Link Load Balance Global Load Balance Web Application Firewall User Authentication

User Authentication

AD FS Proxy

AD FS Proxy

Publish Proxy

Add Filter

Name	Federation Service Name	Status	Availability	AD FS Server Pool
register_58_110	adfs.adfsfortiadc.com	Enable	✓	adfs103

Showing 1 to 1 of 1 entries Show 10 entries

Open the proxy and configure the timeout as customer needed:

Proxy

adfs103\Administrator

Password

Server Configuration Update Interval

300

Default: 300 Range: 1-8640000

Register Timeout

12

Default: 12 Range: 1-3600

Connect Timeout

5

Default: 5 Range: 1-3600

Response Timeout

6

Default: 6 Range: 1-3600

Keepalive Timeout

300

Default: 300 Range: 1-3600

Save Cancel

3.3.2 Configure using scripting

As shown in 3.3.1, when the virtual server uses the AD FS publish service, FortiADC will generate a script at the same time. You can see it in “Server Load Balance->Scripting” page:

Name	
adfs_passthrough_ecp	
adfs_passthrough_owa	
ADFS_passthrough_owa_passthrough-owa_20190103142030	
adfs_publish_ecp	
adfs_publish_owa	
ADFS_publish_owa_publish-owa_20190103143701	
AES_DIGEST_SIGN_2F_COMMANDS	
AUTH_COOKIE_BAKE	
AUTH_EVENTS_n_COMMANDS	
CLASS_SEARCH_n_MATCH	

Upon opening this script, you can get the action that FortiADC will operate. In this script, FortiADC will send the packets to a different backend server pool, which uses content routing. So the customer should add content routings that are the same as the script it is using.

Scripting

Name

ADFS_publish_owa_publish-owa_20190103143701

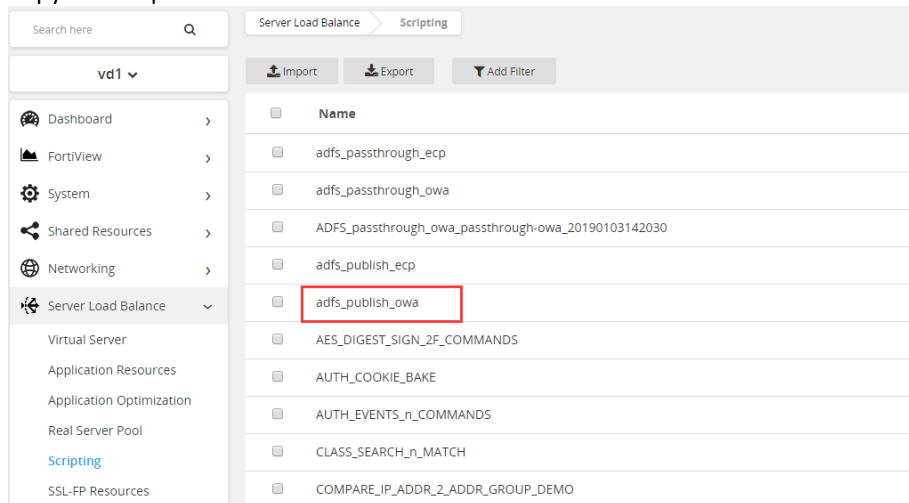
```

1  when RULE_INIT{
2      cookie_name = "EdgeAccessCookie"
3      cookie_value = "ADFS_PROXYCOOKIE"
4      target_cookie = string.format("%s=", cookie_name)
5      pub_uri = "/owa/"
6      external_host = "100.adfsfortiadc.com"
7      internal_uri = "/owa/"
8      internal_domain = "mail.adfsfortiadc.com"
9      adfs_server_domain = "adfs.adfsfortiadc.com"
10     url_redirect="/adfs/ls?version=1.0&action=signin&realm=upn%3AAppProxy%3Acom&appRealm=ea879bbc-d7ca-e811-80b7-001
11 }
12
13 when HTTP_REQUEST{
14     uri = HTTP:uri_get()
15     host = HTTP:header_get_value("Host")
16     path = HTTP:path_get()
17
18     --content-routing
19     --"msapp" "adfsserver" should have created in content-routing module
20     if host:find(external_host) and uri:starts_with(pub_uri) then
21         --redirect
22         cookie_found = 0
23         t={};
24         t["name"]=cookie_name
25         t["parameter"]="value"
26         t["action"]="get"
27         ret = HTTP:cookie(t)
28         if ret then
29             if cookie_value == ret then
30                 cookie_found = 1
31             end
32             --REMOVE this cookie
33             t["parameter"]="cookie"
34             t["action"]="remove"
35             ret = HTTP:cookie(t)
36             if ret then
37                 debug("remove cookie succeed %s\n", ret);
38             else
39                 debug("remove cookie failed\n");
40             end
41         end
42         return_url = string.format("https://%s%s", host, uri)
43         return_url = url_enc(return_url)
44         redirect_url = string.format("https://%s%s", adfs_server_domain, url_redirect)
45         auth_token_invalid = 0
46         if uri:find("authToken=") then
47             --auth_token = get_uri_param(uri, "authToken")
48             --if auth_token_verify(auth_token) then
49                 auth_token_invalid = 1
50             --end
51             HTTP:uri_set(path)
52             --REMOVE all cookies
53             ret = HTTP:cookie_list()
54             for k,v in pairs(ret) do
55                 t["name"]=k
56                 t["parameter"]="cookie"
57                 t["action"]="remove"
58                 ret = HTTP:cookie(t)
59                 if ret then
60                     debug("remove cookie succeed %s\n", ret);
61                 else
62                     debug("remove cookie failed\n");
63                 end
64             end
65         end
66         if cookie_found == 0 and auth_token_invalid == 0 then
67             t={}
68             t["code"] = 307;
69             t["url"] = string.format("%s%s", redirect_url, return_url)
70             HTTP:redirect_t(t);
71         end
72         HTTP:header_replace("Host", internal_domain)
73         LB:routing("exchange102")
74     elseif host:find(adfs_server_domain) then
75         --insert ADFS header
76         cip = IP:client_addr() -- get client ip address
77         HTTP:header_insert("X-MS-Endpoint-Absolute-Path", path)
78         HTTP:header_insert("X-MS-Forwarded-Client-IP", cip)
79         HTTP:header_insert("X-MS-Proxy", "FortiADC")
80         LB:routing("adfs103")
81     else
82         debug("no matches domain for host: %s and uri %s\n", host, uri)
83         HTTP:close()
84     end
85 }
86
87 when HTTP_RESPONSE{
88     location_header = "Location"
89     if HTTP:header_exists(location_header) then
90         location = HTTP:header_get_value(location_header)
91         location_prefix = string.format("https://%s%s", adfs_server_domain, "/adfs/ls/")
92         if location:starts_with(location_prefix) then
93             signout = string.format("%s?wa=wsignout", location_prefix)
94             if location:starts_with(signout) then
95                 insert_cookie = target_cookie
96             else
97                 insert_cookie = string.format("%s%s", target_cookie, cookie_value)
98             end
99             cookie = string.format("%s; Path=%s; Secure; HttpOnly", insert_cookie, pub_uri)
100            HTTP:header_insert("Set-Cookie", cookie)
101        end
102    end
103 }
    
```

Customer can use scripting and content routing instead of AD FS publish service.

Steps:

- (1) Copy this script.



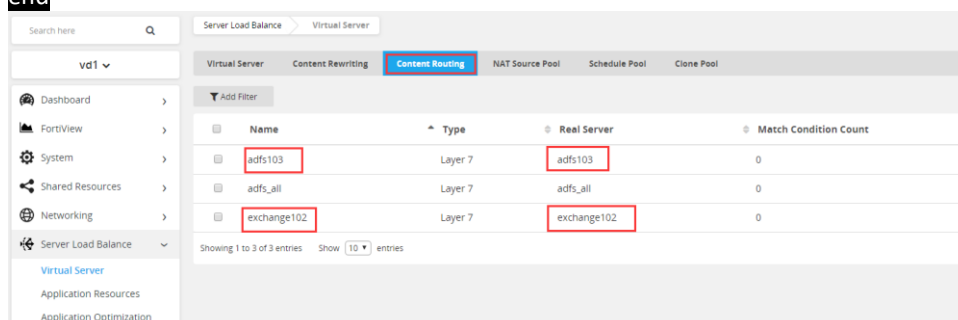
- (2) In virtual server, unset AD FS publish service

```
config load-balance virtual-server
edit "publish_owa"
unset adfs-published-service
next
end
```

- (3) Add content routing

It is the same as that used in the script, like in my example, content-routing "exchange102" using real-server-pool "exchange102", and content-routing "adfs103" using real-server-pool "adfs103"

```
config load-balance content-routing
edit "exchange102"
set load-balance-pool exchange102
config match-condition
end
next
edit "adfs103"
set load-balance-pool adfs103
config match-condition
end
next
end
```



Content Routing

Name

adfs103

Type

Layer 4 Layer 7

General

Schedule Pool

OFF

Real Server Pool

adfs103

Persistence

Click to select

Inherit

Method

Inherit

Content Routing

Name

exchange102

Type

Layer 4 Layer 7

General

Schedule Pool

OFF

Real Server Pool

exchange102

Persistence

Click to select

Inherit

Method

Inherit

- (4) Set the script that was copied in step 1 and in content routing in step 3; set it to the virtual server

```
config load-balance virtual-server
edit "publish_owa"
set type l7-load-balance
set interface port2
set ip 10.58.1.102
set port 443
set load-balance-profile LB_PROF_HTTPS
set client-ssl-profile LB_CLIENT_SSL_PROF_DEFAULT
set content-routing enable
set content-routing-list adfs103 exchange102
set load-balance-method LB_METHOD_ROUND_ROBIN
set scripting-flag enable
set scripting-list ADFS_publish_owa
set traffic-group default
next
end
```

Virtual Server

Basic

General

Security

SSL Traffic Mirror

Application Optimization

Monitoring

Name

passthrough_owa

Type

Layer 7

Layer 4

Layer 2

Status

Disable

Enable

Maintain

Address Type

IPv4

IPv6

Traffic Group

default

Specifics

Content Routing

ON

Content Routing List

Selected Items

adfs103

exchange102

Available Items

Create New

adfs_all

Double-click to deselect. Drag to reorder.

Double-click to select.

Virtual Server

Basic

General

Security

SSL Traffic Mirror

Application Optimization

Monitoring

Configuration

Address

10.58.1.100

Example: 192.0.2.1

Port

443

Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit

0

Default: 0 Range: 0-100000000 concurrent connections

Interface

port2

Public IP Type

IPv4

IPv6

Public IPv4

0.0.0.0

Example: 192.0.2.1

Resources

Profile

LB_PROF_HTTPS

Client SSL Profile

LB_CLIENT_SSL_PROF_DEFAULT

Persistence

Click to select.

Method

LB_METHOD_ROUND_ROBIN

Clone Pool

Click to select

Auth Policy

Click to select

Scripting

ON

To use scripts to manipulate compressed HTTP/HTTPS data body, you must have decompression rules configured first.

Scripting List

Selected Items

adfs_publish_owa

Available Items

adfs_passthrough_ecp

adfs_passthrough_owa

adfs_publish_ecp

passthrough_ecp

Double-click to deselect. Drag to reorder.

Double-click to select.

Save

Cancel

Note:

- When configuring AD FS publish service to the virtual server, FortiADC generates a script. This script will be deleted by the FortiADC when the virtual server unsets AD FS publish service.
- Since AD FS publish uses adfs federation service, the client should configure the mapping between adfs federation service and virtual server ip address, between the external host and the virtual server ip address, such as:
adfs.adfsfortiadc.com 10.58.1.102(virtual server ip)

- 100.adfsfortiadc.com 10.58.1.102(virtual server ip)
Then client requests exchange service: https://100.adfsfortiadc.com/owa/
(3) AD FS publish cannot configure disabled AD FS proxy
(4) Virtual server cannot configure disabled AD FS publish

4 AD FS PROXY DEBUG

4.1 Enable AD FS Proxy debug

- 1) Enable system debug

```
FortiADC-VM # diagnose debug enable
```

- 2) Enable AD FS debug

```
FortiADC-VM # diagnose debug module adfs set
```

4.2 Get AD FS proxy and publish status

- 1) Get adfs proxy status

```
FortiADC-VM # execute adfs-proxy get status register103  
Available
```

- 2) List adfs relyingparty of adfs-proxy

```
FortiADC-VM # execute adfs-proxy get relying-party register103  
{"RelyingParty":["Device Registration Service","ExchangeOWA","ExchangeECP"]}
```

- 3) get adfs publish status

```
FortiADC-VM # execute adfs-publish get status passthrough-owa proxy register103  
Available
```

5 AD FS PROXY TROUBLESHOOTING

5.1 Server Configuration Update Interval

In order to decrease the request to AD FS server when getting an AD FS proxy, or getting publish and relyingpartytrust, a update interval can be configured in AD FS proxy.

Proxy

adfs103\Administrator

Password

Server Configuration Update Interval

300

Default: 300 Range: 1-8640000

Register Timeout

12

Default: 12 Range: 1-3600

Connect Timeout

5

Default: 5 Range: 1-3600

Response Timeout

6

Default: 6 Range: 1-3600

Keepalive Timeout

300

Default: 300 Range: 1-3600

Save

Cancel

Once AD FS proxy is registered to ADFS server and published successfully, FortiADC will cache relyingpartytrust and the status of proxy and publish. During the update interval, even though the customer can receive relyingpartytrust or status, FortiADC will not send requests to AD FS server until update interval timeout.

5.2 AD FS Proxy configuration sync in ha environment

If using AD FS publish service in an HA environment, the configuration and status of AD FS proxy and publish can sync to HA peers. The relyingpartytrust can also sync to HA peers.