SAML 2.0 SSO Deployment with Okta

Simplify Network Authentication by Using Thunder ADC as an Authentication Proxy

Table of Contents

Disclaimer

Overview

The purpose of this deployment guide is to provide detailed instructions on how to deploy SAML 2.0 Authentication using the A10 Networks® Thunder® ADC line of Application Delivery Controllers and Application Access Management (AAM) solution integrated with Okta cloud authentication. The Okta solution is a single sign-on (SSO) solution that integrates with A10 and provides access to backend applications.

Deployment Prerequisites

To deploy the SAML solution with OKTA on A10 Thunder ADC, the following are required:

- ACOS 4.0.1 SP9 or higher
- Thunder ADC supported on hardware, virtual or cloud-based platforms (Azure or AWS)
- Okta SAML subscription (administration credential required)

The A10 Networks SAML 2.0 SSO Deployment with Okta Solution

Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging authentication and authorization data between an Identity Provider (IdP) and a service provider. SAML is a product of the OASIS Security Services Technical Committee. With the introduction of SAML support in A10 Networks Advanced Core Operating System (ACOS®) version 4.0, Thunder ADC can act as a service provider in a security topology and delegate authentication and authorization to IdPs such as Okta. In multi-domain services using the same Identity Provider, SAML offers easy integration and seamless federation with an IdP, even with clients that originate from different service domains.

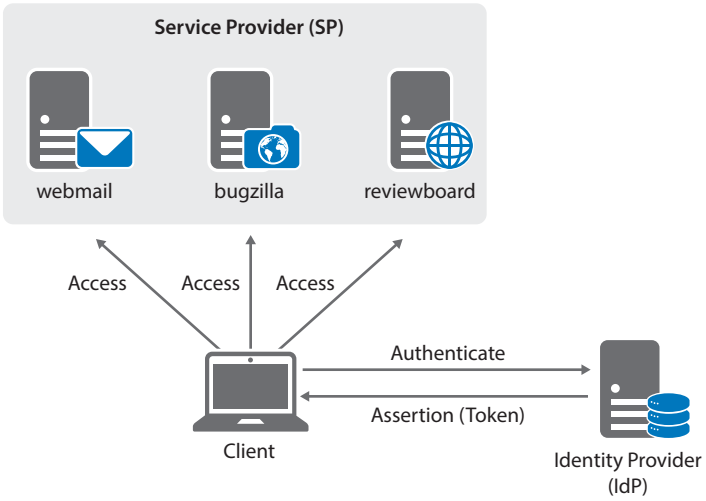

Figure 1: A10 SAML topology

With SAML in ACOS 4.0, the AAM feature plays an important role in protecting resources and distributing access requests. Before access is granted, clients need to provide authentication credentials and meet AAM authorization policies. A security administrator configures an authentication template and an authorization policy in order to perform authentication control. Figure 2 shows an SAML authentication process flow.

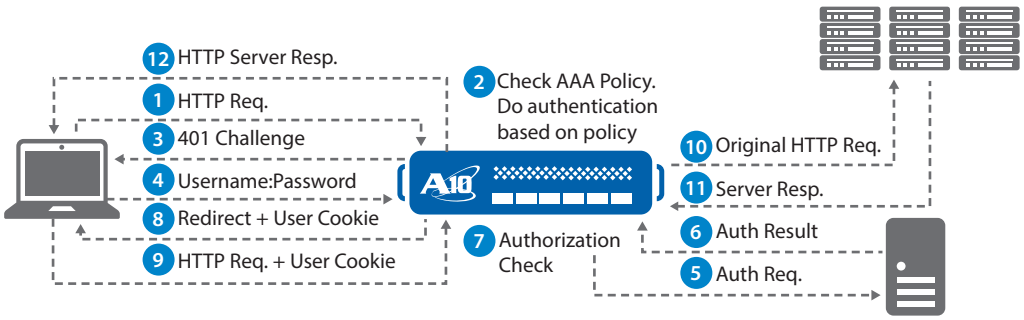

Figure 2: A10 SAML authentication process

Accessing A10 Thunder ADC

Configuring the Thunder ADC Device

The Thunder ADC device provides the following management interfaces:

- Command Line Interface (CLI) – a text-based interface in which commands are entered on a command line. The CLI is directly accessible through the serial console or over the network using either of the following protocols:
  - Secure protocol – Secure Shell (SSH) version 2
  - Unsecure protocol – Telnet (if enabled)
- Graphical User Interface (GUI) – web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

***Note**: HTTP requests are redirected to HTTPS by default on the Thunder ADC device.*

By default, Telnet access is disabled on all interfaces, including the management interface. SSH, HTTP and HTTPS are enabled by default on the management interface only and disabled by default on all data interfaces.

Logging into the CLI

Thunder ADC provides advanced features for securing management access to the SSH client device. This section assumes that only the basic security settings are in place.

To log into the CLI using SSH:

- On a PC connected to a network that has access to a dedicated management interface, open an SSH connection to the IP address of the management interface.

***Note**: The default IP address is 172.31.31.31*

- Generally, if this is the first time the SSH client has accessed the Thunder ADC device, the SSH client displays a security warning. Read the warning carefully, then acknowledge the warning to complete the connection. Click on Enter.
- At the "login as:" prompt, enter the username "admin."

  At the "Password:" prompt, enter the admin password. The default password is "a10." If the admin username and password are valid, the command prompt for the User EXEC level of the CLI appears as ACOS>.
- The User EXEC level allows you to enter a few basic commands, including some show commands as well as ping and traceroute.
- To access the Privileged EXEC level of the CLI and allow access to all configuration levels, enter the "enable" command. At the "Password:" prompt, enter the enable password as blank; then press Enter.

***Note**: This is not the same as the admin password, although it is possible to configure the same value for both passwords.*

- If the enable password is correct, the command prompt for the Privileged EXEC level of the CLI appears as "Thunder#."
- To access the global configuration level, enter the "config" command. The following command prompt appears as "Thunder(config)#."

***Note**: See the Thunder Series Configuration Guide, or the Thunder Series System Configuration and Administration Guide and Application Delivery and Server Load Balancing Guide, for additional features and functions of the Thunder ADC device.*

Logging onto the GUI

To log onto the GUI:

- In your web browser, enter the HTTPS request with the management IP address of the Thunder ADC device (https://management-IP-address/). A logon dialog is displayed.

***Note**: Dialog name and display image are different depending on the browser and browser version you are using. In this example, the Firefox browser is being used.*

Figure 3: ACOS GUI login dialog

Since there is no root certificate for Thunder ADC's internal Certificate Authority(CA), which issues web server certificates for a management site on access PCs, warnings or alert messages are shown upon first accessing the device. When the security exception process is done, the login prompt shown in Figure 3 will appear.

***Note**: For the default admin credentials, the username is "admin" and the password is "a10."*

- Enter your admin username and password and click OK.
- The Summary page will appear showing at-a-glance information for your Thunder ADC device. You can access this page again at any time while using the GUI, by navigating to **Monitor > Overview > Summary**.

Okta Initial Setup

One of the requirements for Okta SAML authentication is that the administrator must have access to the Okta Management Console.

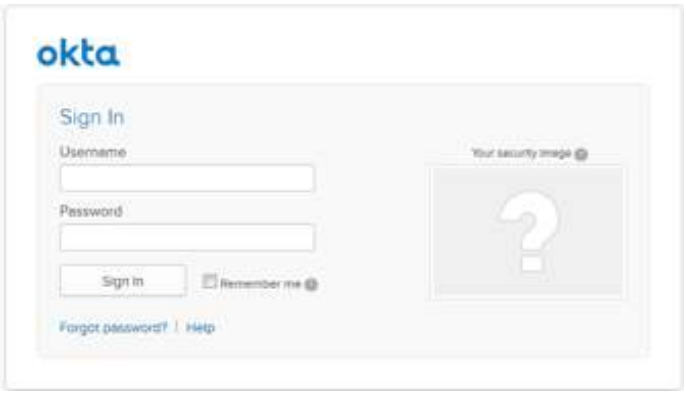

Figure 4: Okta GUI login dialog

Login with the proper credentials and navigate through the interface Okta under **Applications > Add Application > Create New App**.

Under the general settings, enter the following items:

Application label: "A10 Networks"

Force Authentication: "Unselected"

Post back URL: http://192.168.2.100/api/SsoAuthLoginResponse

***Note**: Post back URL will match the entity ID and the Assertion Consumer Services (ACS) URL of the A10 Thunder ADC device.*

Name ID Format: This option is selectable and the default is "email address"

Recipient: Same as Post back URL

Audience restriction: http://192.168.2.100 (equal to the entity ID)

authnContectClassRef: Select "PasswordProtectedTransport"

Response: Select "signed"

Assertion: Select "signed"

Request: Select "compressed"

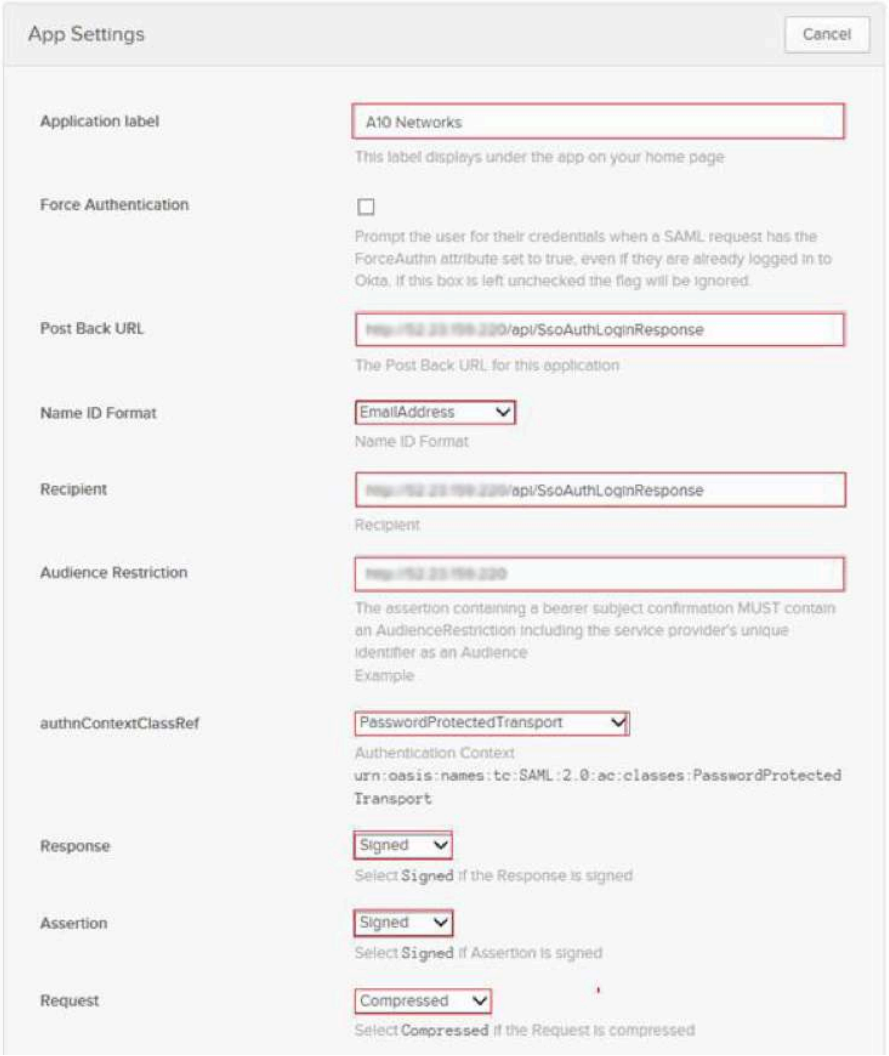

Figure 4: Okta new application settings

Figure 5: Okta additional application settings

Destination: http://192.168.2.100/api/SsoAuthLoginResponse

***Note**: Post back URL will match the entity ID and ACS URL of the Thunder ADC device.*

Default relay state: Can be any or blank

***Note**: This is used in IdP initiated SSO post; if no value is set, Relay State is sent.*

Attribute statements, Group Name and Group Filter will be blank. Application visibility will be unselected. Save configuration and the application will be added to the application list. Once this is configured, the application that was just created should be "active."

VPN Notification: VPN Required Notification: Disabled

Figure 6: Okta VPN notification option

App Embed Link: No modification required

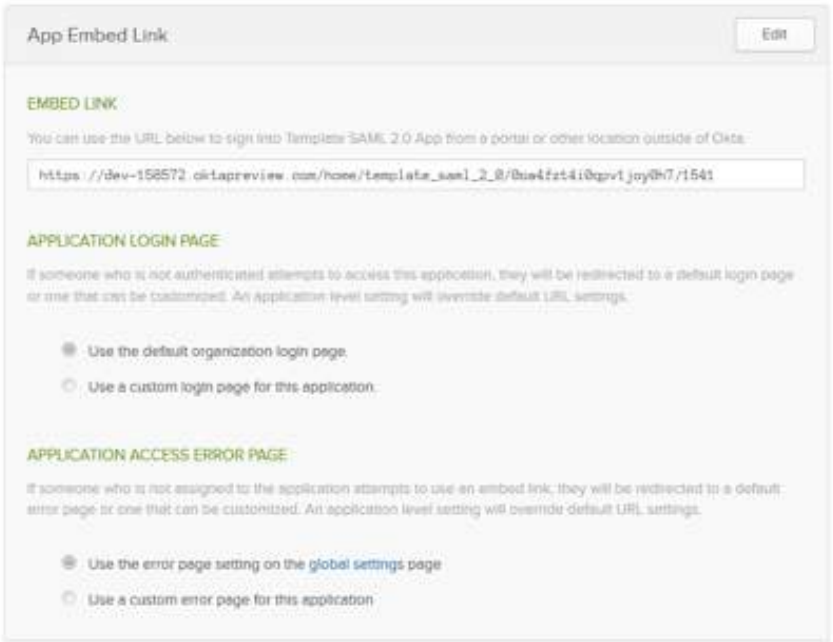

Figure 7: App embed link

Okta Sign On Configuration

This next step is to configure the Sign On section of Okta. To navigate to this section, go to **Applications > Select the Application > Sign On**.

In the Sign On section, download the "Identity Provider metadata" file. Save this file for future configuration. For additional installation and deployment steps, view setup instructions.

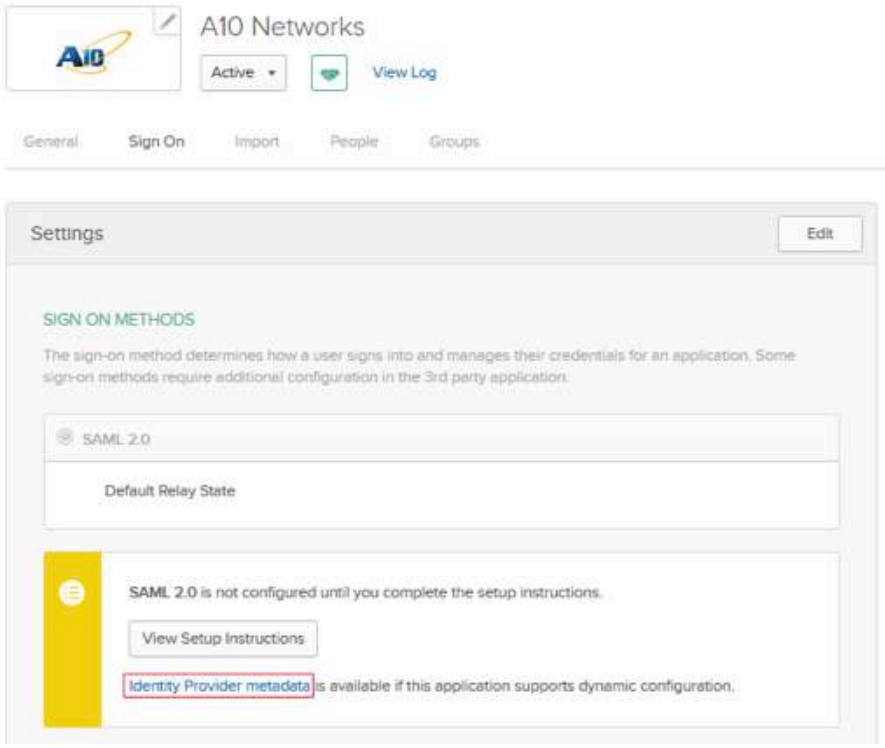

Figure 8: Okta sign on methods settings

***Note**: Once the metadata is downloaded, the metadata file has to be imported to the Thunder ADC device. This uploads the file.*

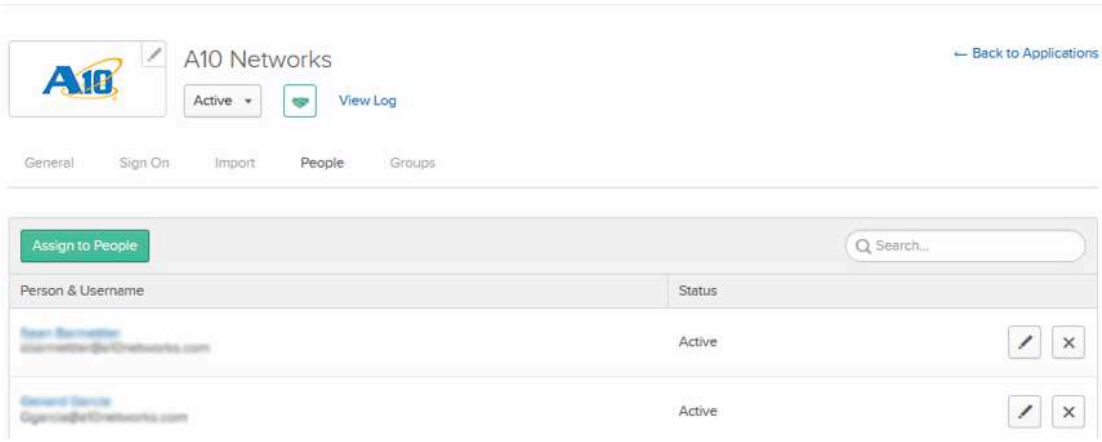

Figure 9: Okta user list

***Note**: Users can be imported using a .csv file. Make sure you use the correct import template for users to be imported correctly in the Okta portal. The instructions on how to import users are available in the "import" tab of the Okta management console.*

Navigate to the Sign On Policy and create a policy rule as follows:

Rule name: Signon

Under Conditions, define as follows:

People: User assigned this app

Location: Anywhere

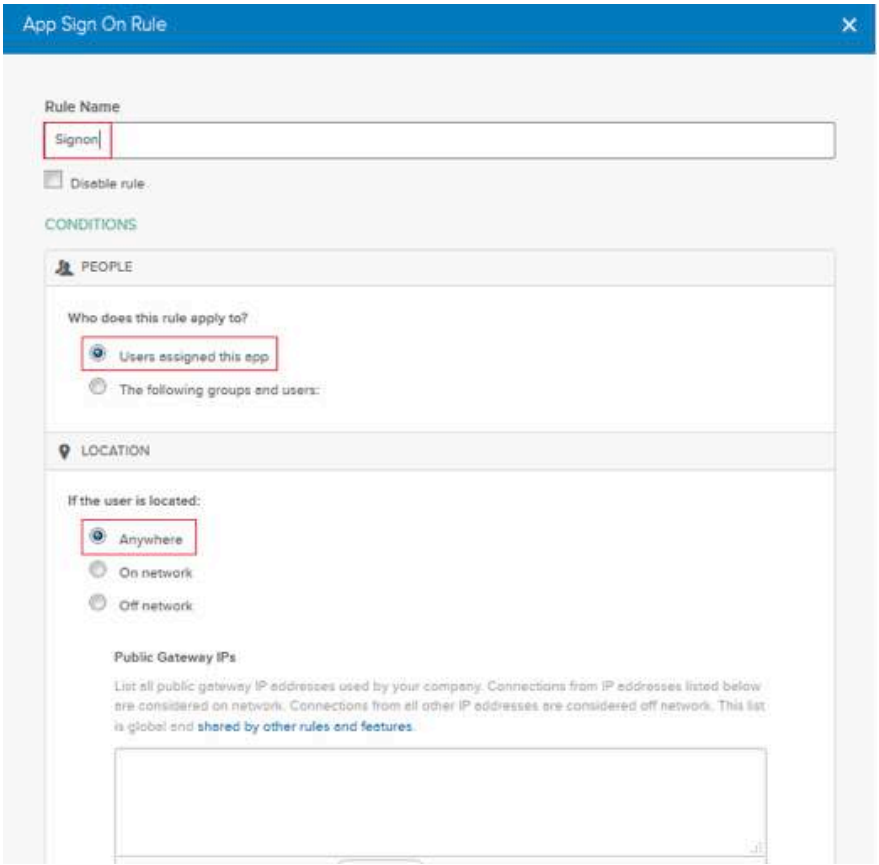

Figure 10: Okta app sign on rule

For access policy, you can define either an Allowed or Denied access. In this case, we will select Allowed to allow users to access the A10 application.

***Note**: "Prompt for re-authentication" is an option to request within a specific timeframe. This feature defaults to 60 minutes.*

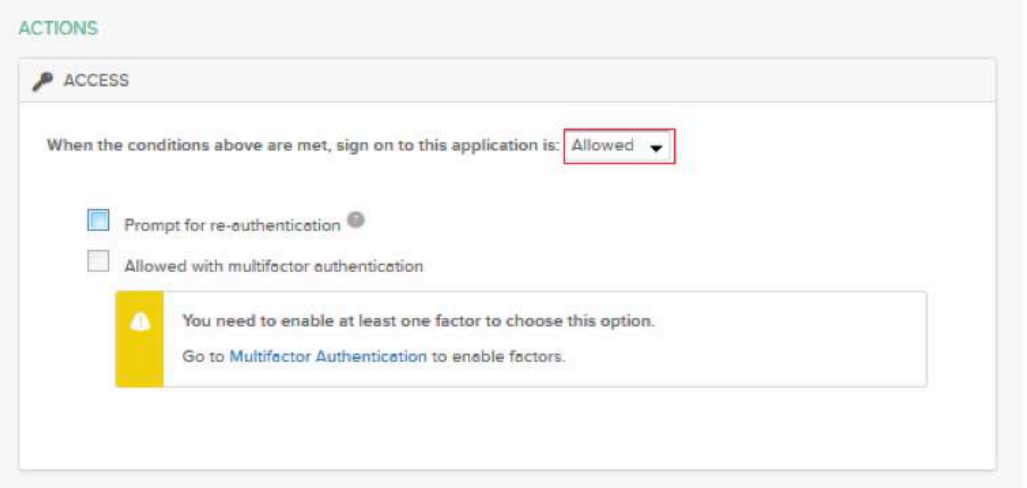

Figure 11: Okta access permissions

A10 Thunder ADC AAM Configuration for Okta SAML 2.0

Note: The sample configuration included in this section is based on cloud-based solutions in AWS or Azure deployments. Note that some settings will need to be modified depending on your environment.

- AAM Authentication SAML configuration (service provider)
  - Service provider name must be defined (i.e., Okta-sp).
  - Assertion-consuming-service location must be defined with this parameter "/api/SsoAuthLoginResponse" and you also need to create a unique index number.
  - Binding post
  - Entity-ID and Service-URL are identical and both configurations are required in ACOS.
- AAM Authentication SAML configuration (Identity Provider)
  - Identity Provider name must be defined (i.e., Okta-idp).
  - Metadata "Okta mdata" must be uploaded. Refer to section on how to download the metadata information.
- AAM Authentication template
  - Authentication template type must be defined as "SAML."
  - SAML-SP name must be defined in this section (i.e., "okta-sp").
  - SAML-IDP name must be defined in this section (i.e., "okta-idp").
- AAM Authorization Policy
  - Create an SAML Authorization Policy
  - Define AAA policy with Allow or Deny
  - Add the authentication template
- AAA policy
  - Bind the AAA Policy in the VIP

A

```
multi-config enable
!
web-service axapi-timeout-policy idle 60
web-service port 8081
web-service secure-port 8443
!
interface ethernet 1
  ip address dhcp
!

ip nat pool aws-nat1 192.58.100.100 192.58.100.100 netmask /24
!
health monitor aws-tcp-probe
  method tcp port 80
!
```

B

```
aam authentication saml service-provider okta-sp
  assertion-consuming-service index 0 location /api/
SsoAuthLoginResponse binding post
  entity-id http://192.168.2.100
  service-url http://192.168.2.100
!
```

C

```
aam authentication saml identity-provider okta-idp
  metadata okta_mdata
!
slb server aws-www 192.0.2.10
  health-check aws-tcp-probe
  port 80 tcp
!
```

D

```
aam authentication template okta1
  type saml
  saml-sp okta-sp
  saml-idp okta-idp
!
```

E

```
aam authorization policy saml_test
!
aam aaa-policy okta-policy
  aaa-rule 1
    action allow
    authentication-template okta1
!
      slb service-group aws-www tcp
  health-check aws-tcp-probe
  member aws-www 80
!
```

F

```
slb virtual-server aws-www use-if-ip ethernet 1
  port 80 http
    name aws-www_80_tcp
    source-nat pool aws-nat1
    service-group aws-www
    aaa-policy okta-policy
!
      end
!Current config commit point for partition 0 is 0 & config mode is
classical-mode
vThunder#
```

Note: *The Entity-ID and Service URL will have the same IP address as the VIP address. The sample configuration is based on AWS EC2, so the Service URL and Entity-ID will be based on the AWS Dynamic Host Configuration Protocol (DHCP) address (e.g., 192.168.2.100).*

Concept of Authentication and Authorization

The A10 AAM solution supports authentication and authorization using SAML. With SAML authentication, SAML authorization is configured as part of the AAA policy that is bound within the vPort (in other words, server load balancing virtual server configuration).

The first step is to create AAA rule/s that can provide a criteria for what can be accessed. Define "allow" or "deny" access, deploy an authentication template and provide an authorization policy. Finally, once the policy is configured, bind it within the vPort for the AAA policy to take effect. The sample configuration in Figure12 shows this in more detail.

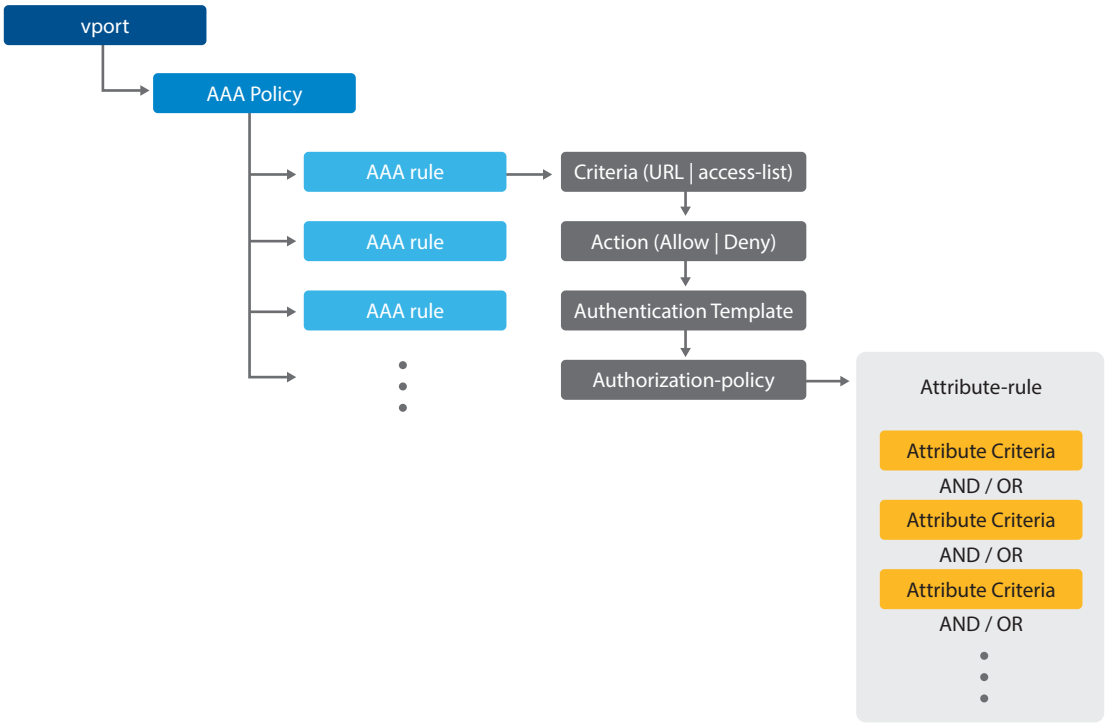

Figure 12: A10 AAA policy configuration

Each AAA policy will include the following:

- **Criteria**: User can configure access list, URI or domain name as criteria to associate client requests to this rule.
- **Action**: Action to perform (allow or deny) after client request is associated to this rule.
- **Authentication template**: This applies if client request is allowed access via the AAA rule. The authentication template per¬forms authentication for the user of the request.
- **Authorization policy**: If client authentication is successful, ACOS can also perform authorization to check whether the authenticated user has permission to access the requested resource.

A10 SAML Commands

Here's a list of the most common commands specific to SAML configuration:

- show aam authentication saml idp- command: Shows the SAML Identity Provider settings
- show aam authentication saml sp- command: Shows the SAML service provider settings
- show aam authentication saml sp-session- command: Show the SAML service provider sessions
- show aam authentication statistic- command: Shows all AAM statistics including Kerberos, RADIUS, NTLM-Relay, SAML and others. This command provides the detailed statistics of an SAML session.

A10 SAML Session Sample

Figure 13 shows sample CLI outputs for an SAML authentication session and a service provider session.

```
vThunder#show aam authentication session
 TTL = Session Idle timeout (Sec), Lifetime = SAML Token/Assertion Lifetime (Sec)
Total Sessions: 1
------------------------------------------------------------------------------
ID      Type   VIP             User            Client IP       Created Time
       VPort  Domain          Domain-group    TTL             Lifetime
------------------------------------------------------------------------------
2       SAML   aws-www         111@example.com 192.48.114.162  15-10-15 13:15:28
       80                     0               272             375

vThunder#show aam authentication saml sp-session

Service Provider: okta-sp
NameID          Client addr          Id Provider                                Auth
Instant                Expiration time
------------------------------------------------------------------------------------
----------------------------------------
111@example.com 192.48.114.162       http://www.okta.com/exk4fzt4hzujIyuna0h7   2015-10-
15T12:15:27.148Z     2015-10-15 13:22:27
vThunder#
```

Figure 13: A10 SAML authentication session

Figure 14 shows a sample of AAM authentication statistics. Note that when you issue this command on the ACOS CLI, other AAM statistics will come out, including Kerberos, NTLM relay, OCSP and others. The SAML statistic is just a portion of the CLI output.

```
vThunder#show aam authentication statistics
SAML statistic:
-----------------------
SP metadata export requests: 0
SP metadata export successes: 0
Login authn requests: 20
Login authn responses: 0
SSO requests: 0
SSO successes: 15
SSO authorization failed: 2
SSO errors: 0
SLO requests: 0
SLO succeses: 10
SLO errors: 0
Other errors: 0
```

Figure 14: A10 authentication statistics

Summary

In summary, the configuration steps described in this deployment guide show how to set up Thunder ADC AAM integration with the Okta cloud SAML solution. With the introduction of SAML support in ACOS version 4.0, this integrated solution provides the following benefits:

- Minimizes the overwhelming nature of user interactions with traditional AAA servers
- Simplifies network authentication by using the A10 device as an authentication proxy
- Offloads web and authentication servers
- Enables Thunder ADC devices to handle the sending and initial processing of authentication challenges, forwarding credentials to SAML IdP and granting access

By using A10 Thunder ADC, significant benefits are achieved for all authentication deployments.

For more information about A10 Thunder ADC products, please refer to the following URLs:

www.a10networks.com/products/thunder-series/thunder-application_delivery_controller

www.a10networks.com/products/application-delivery-controllers

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DG-16155-EN-01
Dec 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
HongKong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.