Cisco Application Centric Infrastructure and Symantec Validation and ID Protection: Use and Configuration

What You Will Learn

Cisco® Application Centric Infrastructure (ACI) offers detailed role-based access control (RBAC) and authentication and can integrate with Symantec Validation and ID Protection (VIP) Services to help enable enterprises secure access and online transactions to meet compliance and standards requirements and reduce the risk of security breaches.

Challenges

The working environments of many organizations are evolving in response to factors such as the growth of the mobile workforce, the increasing use of cloud-based applications, and the expansion of bring-your-own-device (BYOD) initiatives. The greater flexibility that mobility offers means more opportunity, but also new challenges. Information technology staffs are still tasked with meeting the traditional challenges they have always faced: protecting against breaches when data and applications are accessed (remotely or locally) and complying with industry regulations that help ensure protection. But they now also face a new set of challenges, such as the need to provide mobile employees with a simple, yet secure, user experience. Organizations can meet these challenges by implementing strong, smarter authentication to secure their enterprise data and applications while also offering greater ease of use.

Business Benefits of the Cisco and Symantec Solution

An excellent solution to meet the evolving needs of IT departments and users is two-factor authentication (2FA). 2FA authentication is a proven tool to protect against unauthorized access to enterprise applications and data, both in the enterprise network and in the cloud. 2FA demands something a user knows (such as a user name and password) and something a user has (a hardware credential such as a token, a smartcard, a cell phone, or, in a tokenless implementation, a device or a behavioral profile). For enterprises, this dual mechanism delivers a higher level of security to protect confidential data and applications while meeting compliance requirements.

Symantec VIP provides an additional layer of protection beyond the standard user name and password through a wide variety of other authentication capabilities. Cisco ACI integration was validated using strong authentication with a security code. The VIP strong authentication platform provides dynamic, one-time-use security codes generated by a user's VIP credentials in the form of mobile apps (Cisco validated), desktop software, security tokens, and security cards. When a user logs into the Cisco Application Policy Infrastructure Controller (APIC) using the security code generated by the Symantec VIP Access app on the user's mobile device, the login is passed to the Symantec VIP Enterprise Gateway RADIUS server. The RADIUS server validates the security code in the Symantec VIP Services, and the user password in the enterprise Lightweight Directory Access Protocol (LDAP) data store.

Cisco ACI

Cisco ACI uniquely addresses the security needs of the next-generation data center with an application- centric approach and a common, policy-based operations model, while helping ensure compliance and reduce the risk of security breaches. ACI delivers segmentation, such as tenant-level isolation, that is dynamic and application centered as well as detailed RBAC and secure user authentication.

ACI provides multitenant isolation and prevents information privacy from being compromised across tenants. Read-write restrictions prevent any tenant from seeing any other tenant's configuration, statistics, faults, or event data. Unless the administrator assigns permissions to do so, tenants are restricted from reading fabric configuration, policies, statistics, faults, and events.

Cisco APIC policies manage the access, authentication, and accounting (AAA) functions of the ACI fabric. The combination of user privileges, roles, and domains with access rights inheritance enables administrators to configure AAA functions at the managed-object level in a very detailed way. These configurations can be implemented using the Representational State Transfer (REST) API, the command-line interface (CLI), or the GUI.

The APIC supports both local and external authentication and authorization (TACACS+, RADIUS, and LDAP) as well as RBAC to control read and write access for all managed objects and to enforce ACI administrative and per-tenant administrative separation.

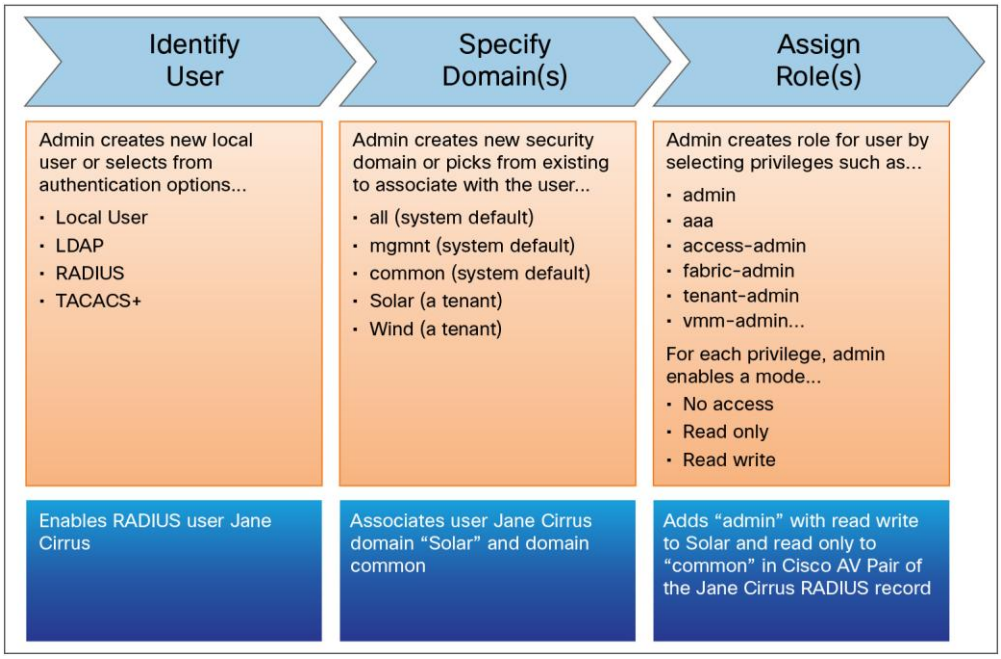
The APIC provides access according to a user's role through RBAC. An ACI fabric user is associated with the following:

- A set of roles
- For each role, a privilege type: no access, read-only, or read-write
- One or more security domain tags that identify the portions of the management information tree (MIT) that the user can access

The APIC requires that an administrator configure a Cisco attribute-value (AV) pair on an external authentication server. To do so, the administrator adds a Cisco AV pair to the existing user record. The Cisco AV pair specifies the RBAC roles and privileges for the user that the APIC requires. The Cisco AV pair format is the same for RADIUS, LDAP, and TACACS+.

Figure 1 provides an overview of ACI authentication.

Figure 1: Cisco ACI Authentication



For more information about Cisco ACI, see the references at the end of this document.

Symantec VIP

Sophisticated network attacks have rendered simple password authentication insufficient to protect an organization against unauthorized access to its network and applications. The ramifications of unauthorized access to confidential information are dire: noncompliance, financial penalties, and theft of intellectual property.

Symantec VIP is a leading user-friendly, cloud-based, strong authentication service that enables enterprises to secure access to networks and applications. It augments password-based logins with an additional layer of authentication, such as intelligent authentication or a hardware, software, or mobile credential.

VIP's broad array of authentication options allows an organization to select the right authentication approach to deliver protection for a variety of users and use cases. Options range from traditional one-time password (OTP) credentials to device ID and risk-based analysis to invisibly authenticate known users exhibiting expected login behavior, or a combination of both.

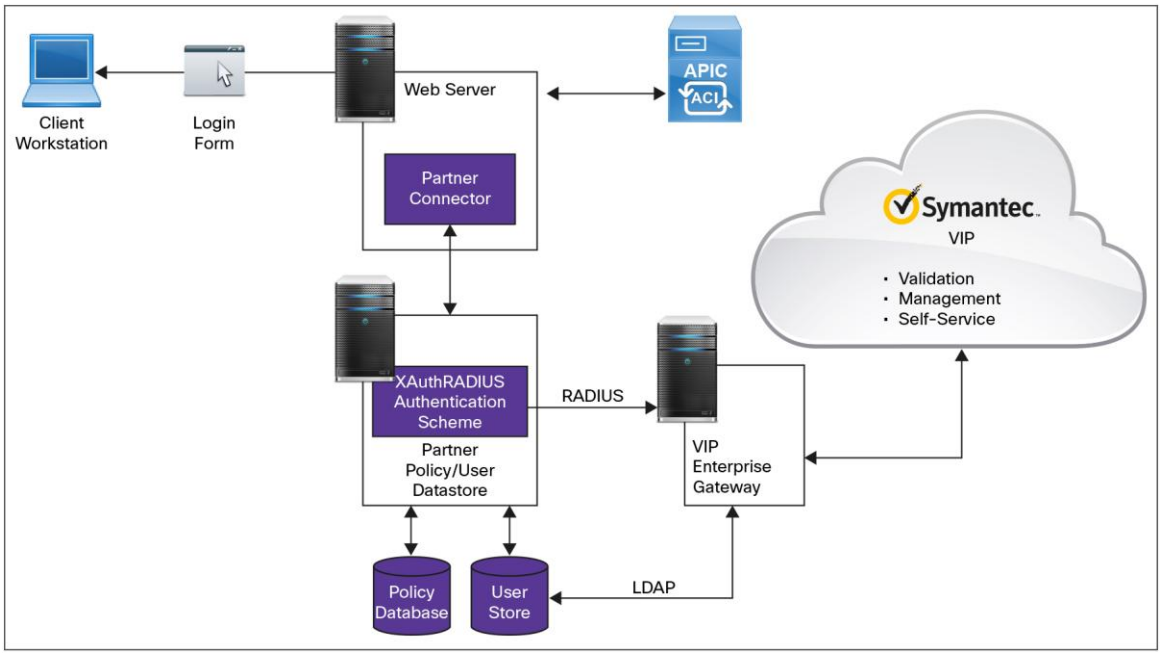
Attackers constantly change tactics, and it's important to have an authentication solution that can address these challenges, both now and in the future. The VIP cloud-based approach enables easy delivery of new capabilities as well as integration with the Symantec Global Intelligence Network, allowing you to stay ahead of emerging threats.

In addition, VIP is designed to integrate easily with popular enterprise VPNs, web mail, single-sign-on (SSO) applications, and enterprise directories, such as the solutions provided by ACI, to make access easy and secure.

Integration Overview

Figure 2 shows the topology of the Cisco and Symantec solution.

Figure 2: Topology



The solution assumes that the following components are operational and in a ready-to-use state:

- Cisco ACI fabric
- Microsoft Active Directory
- Symantec VIP Gateway
- Symantec VIP Mobile on smartphone

Hardware and Software Used

The Cisco integration validation used the products listed here. Cisco supports several other switch options in ACI mode, all of which are capable of integration with Symantec VIP. For more information about other Cisco Nexus® 9000 Series Switches hardware platforms for ACI, refer to the following data sheet: http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/application-policy-infrastructure-controller-apic/datasheet-c78-732414.html.

Detailed system requirements for various Symantec VIP components can be found at http://www.symantec.com/en/in/vip-authentication-service/system-requirements/.

- Cisco ACI part numbers
  - 2 x N9K-C9508
  - 2 x N9K-X9736PQ
  - 1 x APIC-CLUSTER-M1
  - 1 x N9K-C9396PX
  - 1 x N9K-C93128TX
  - 8 x BiDi optics module (QSFP-40G-SR-BD)
  - 2 x Cisco ACI software licenses for 48-port 1/10-Gbps Cisco Nexus 9000 Series Switches (ACI-N9K-48X)
- Cisco APIC Release 1.0(3i) image
  - aci-apic-dk9.1.0.3i.iso
- Cisco Nexus 9000 Series ACI Mode Software Release 11.0(3i)
  - aci-n9000-dk9.11.0.3i.bin
- LDAP
  - Active Directory on Microsoft Windows Server 2003
- Symantec VIP Enterprise Gateway minimum hardware requirements
  - Intel or Intel-compatible 32-bit or 64-bit architecture
  - 2 GB of RAM
  - 10 GB of disk space
- Symantec VIP Access for Mobile application running on iOS, Android, Microsoft Windows Phone 8.0, Blackberry, or other mobile OS

Symantec VIP System Configuration

Performing Preconfiguration

Be sure that the VIP environment is set up properly before you proceed with the integration.

1. If you do not have a Symantec VIP account, you can request a trial account by going to http://www.symantec.com/en/in/vip-authentication-service/ and clicking the Trialware link in the Next Steps section.
2. Download and review the VIP Enterprise Authentication Deployment Guide from VIP Manager. The document can be found by choosing Account Tab > Download Files link > General Documents.
3. Verify that you a have VIP Enterprise Gateway set up and configured to communicate with the Symantec VIP Services using your account credentials. For details about this configuration, follow the steps documented in the VIP Enterprise Gateway Installation and Configuration Guide. The software and all associated documents can be downloaded from the VIP Manager Account tab by choosing Enterprise Gateway and selecting the version number.

Creating a User in Symantec VIP

A user account can be created in Symantec VIP, and a VIP credential can be bound to the account using one of the following methods:

- The administrator can create a user account using the VIP Manager.
- The user account can be automatically populated from the enterprise LDAP data store.
- The user can bind the VIP credential by logging into a VIP self-service portal.

For testing purposes, the first option is used here.

1. Log in to the VIP Manager by providing your administrator email ID and password.
2. Click the Users tab.
3. Click the Add New User link in the top right corner.
4. Provide the user name you will typically use in your enterprise LDAP directory to log in. The same user must exist in your enterprise LDAP directory.
5. In the Credential section, select VIP Credential.
6. Provide the Credential ID information from the VIP Access application installed on your smartphone.
7. Provide a friendly name for the credential.
8. Click Add to complete the user creation.

You can now use the created user account for subsequent user authentication testing.

Configuring the LDAP User Store

If you have the user information available in an enterprise LDAP directory such as Microsoft Active Directory, configure it in the VIP Enterprise Gateway as a user store.

1. Login to the VIP Enterprise Gateway administration console.
2. Go to the User Store tab and click the Add a User Store link.
3. Provide the LDAP server connection information such as the host IP address and port details.
4. Provide the administration user account used to access the LDAP data store for querying as well as the password for the same.
5. Provide the base domain name and user filter that will be used to search users in the LDAP database for authentication of users in VIP Enterprise Gateway.
6. Provide a test user to be searched in the configured user filter and verify that the user can be found by clicking the Test button.
7. After the test succeeds, submit the form to complete the user store configuration.

The configuration concepts and steps are detailed in the section “Configuring User Stores” in the VIP Enterprise Gateway Installation and Configuration Guide as well as in the online help available with the VIP Enterprise Gateway.

Configuring the RADIUS AAA Server

You can configure a validation server in the VIP Enterprise Gateway that will act as a RADIUS AAA server for authentication. VIP Enterprise Gateway currently supports RADIUS Password Authentication Protocol (PAP) as the authentication protocol.

1. Log in to the VIP Enterprise Gateway administration console.
2. Go to the Validation tab and select the User ID + LDAP Password + Security Code mode of validation when adding a validation server.
3. Provide the following information to configure the server:
    a. Server name for unique identification
    b. Host IP address and port to listen to RADIUS messages over User Datagram Protocol (UDP)
    c. RADIUS shared secret to encrypt the RADIUS messages on the wire; make sure you provide the same value when you configure a RADIUS AAA client
    d. RADIUS-to-LDAP mapping

        This feature is relevant if you are planning to provide additional attributes to the AAA clients upon successful authentication for user authorization. In this configuration, the Cisco AVPair attribute has been used to enable specific functions of the APIC console.

        i. Select Vendor Specific as the RADIUS mapping attribute.
        ii. For Vendor Id, select Cisco.
        iii. For Attribute Id, enter **1.**

iv. For Attribute Type, select String.

v. Test with a specific user to verify that the attributes are returned properly from the LDAP data store.

4. Submit the form to complete the validation server configuration.
5. Start the validation server

The configuration concepts and steps are detailed in the section “Configuring Validation Services” in the VIP Enterprise Gateway Installation and Configuration Guide as well as in the online help available with the VIP Enterprise Gateway.

Testing the RADIUS AAA Server

Use the <VIP_MAUTH_HOME>/tools/vsradiuseclient_test tool to verify that your RADIUS client functions properly. This tool sends an authentication request to the VIP Validation Service. Use the user created earlier in VIP Manager to authenticate with this test tool.

Here is the usage information for the tool:

./vsradiusclient_test --server-host <server name/ip address> --server-port <server port> --client-ip <ip address> --secret <radius shared secret> --user-name <username> --password <LDAP Password + OTP> --verbose --timeout <60>

On successful authentication, you will receive a RADIUS access response with all the configured RADIUS attributes. Detailed explanations of the tool, parameters, and sample commands can be found in the chapter “Testing the Installation” in the VIP Enterprise Gateway Installation and Configuration Guide.

Cisco APIC System Configuration

Configuring Cisco APIC as a RADIUS Client

1. From the Cisco APIC GUI, click the Admin tab at the top of the screen.
2. Select AAA in the subpane.
3. In the left pane, click RADIUS Management.
4. Right-click RADIUS Provider and choose Create RADIUS Provider.
5. Enter the IP address of the RADIUS server (the validation server running on Symantec VIP Enterprise Gateway).
6. Verify that the authorization port matches the port configured on the validation server of Symantec VIP Enterprise Gateway.
7. Select PAP as the authorization protocol.
8. Click Submit.
9. Right-click RADIUS Provider Groups and select Create RADIUS Provider Group.
10. Enter a name for the RADIUS provider group and an optional description.
11. Click the plus sign under Providers and add the RADIUS server configured previously.
12. Click Submit.

Enabling RADIUS Authentication on Cisco APIC

1. From the Cisco APIC GUI, click the Admin tab at the top of the screen.
2. Select AAA in the subpane.
3. In the left pane, choose AAA Authentication > Login Domains.
4. Right-click Login Domain and choose Create Login Domain.
5. Enter a name for the login domain and, optionally, a description.
6. From the Realm drop-down menu, choose RADIUS.
7. Click Submit.
8. In the left pane, click the new domain previously created under Login Domain.
9. In the center pane, choose the previously created RADIUS provider group in the drop-down menu.

Configuring Microsoft Active Directory

1. Right-click the name of the user.
2. Click CiscoAVPair:
    a. Shell:domains=all/admin/common/read-all
    b. You can change the role and domain by updating the field below “Entering the IFC authorization roles and domains here.”

Now Cisco ACI is configured for strong two-factor authentication using the Symantec VIP Access app for mobile devices and Symantec VIP Enterprise Gateway.

Cisco Verification

1. Log in to the APIC.
    a. Username: Use Active Directory User.
    b. Password: Use Active Directory Password + One Time Password from Symantec VIP Access App.
    c. Domain: From the drop-down menu, choose Radius.
2. Verify that the user has the correct RBAC information.

Verification on Symantec

Because a RADIUS AAA server is used, most of the Symantec verification is performed in the back-end logs.

1. Log in to the VIP Enterprise Gateway administration console.
2. Select the Logs tab.
3. Click the server logs and select the log for the specific validation server configured.
4. Look in the log statements for the status of the last login attempt to determine whether the authentication was successful.

For More Information

- Cisco ACI: http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html
- ACI security documentation: http://www.cisco.com/c/en/us/solutions/enterprise-networks/application-centric-infrastructure-security/index.html
- Cisco ACI configuration guide: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/aci-fundamentals/b_ACI-Fundamentals/b_ACI_Fundamentals_BigBook_chapter_0110.html
- Symantec VIP overview: http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-21213686-2_GA_DS-Validation-and-ID-Service-0714.pdf

C11-734458-00 06/15