CHAPTER 5

Configuring Role-Based Access Control

This chapter describes how to configure role-based access control (RBAC) on the Cisco 4700 Series Application Control Engine (ACE) appliance. It describes how to create a domain and a user, and how to associate the user with a predefined role and the new domain.

This chapter contains the following sections:

- Information About Role-Based Access Control
- Configuring RBAC
- Configuration Example for Configuring RBAC
- Where to Go Next

Information About Role-Based Access Control

After reading this chapter, you should have a basic understanding of how the ACE appliance provides security administration by using RBAC and how to configure a server maintenance user with permission to access a subset of your network.

One of the most challenging problems in managing large networks is the complexity of security administration. The ACE appliance allows you to determine the commands and resources available to each user through RBAC. In RBAC, users are associated with domains and roles.

A domain is a collection of physical and virtual network resources such as real servers and virtual servers.

User roles determine a user's privileges, such as the commands that the user can enter and the actions the user can perform in a particular context. The ACE provides a number of predefined roles. In addition, administrators in any context can define new roles.

The ACE provides the following predefined roles, which you cannot delete or modify:

- Admin—If created in the Admin context, has complete access to, and control over, all contexts, domains, roles, users, resources, and objects in the entire ACE. If created in a user context, gives a user complete access to and control over all policies, roles, domains, server farms, real servers, and other objects in that context.
- Network Admin—Has complete access to and control over the following features:
  - Interfaces
  - Routing
  - Connection parameters

  - Network Address Translation (NAT)
  - VIPs
  - Copy configurations
  - **changeto** command
  - **exec** command
- Network-Monitor—Has access to all **show** commands and to the **changeto** and **exec** commands. If you do not explicitly assign a role to a user with the **username** command, this is the default role.
- Security-Admin—Has complete access to and control over the following security-related features within a context:
  - ACLs
  - Application inspection
  - Connection parameters
  - Interfaces
  - Authentication and accounting (AAA)
  - NAT
  - Copy configurations
  - **changeto** command
  - **exec** command
- Server-Appln-Maintenance—Has complete access to and control over the following features:
  - Real servers
  - Server farms
  - Load balancing
  - Copy configurations
  - **changeto** command
  - **exec** command
- Server-Maintenance—Can perform real server maintenance, monitoring, and debugging for the following features:
  - Real servers—Modify permission
  - Server farms—Debug permission
  - VIPs—Debug permission
  - Probes—Debug permission
  - Load balancing—Debug permission
  - **changeto** command—Create permission
  - **exec** command—Create permission
- SLB-Admin—Has complete access to and control over the following ACE features within a context:
  - Real servers
  - Server farms
  - VIPs

  - Probes
  - Load balancing (Layer 3/4 and Layer 7)
  - NAT
  - Interfaces
  - Copy configurations
  - **changeto** command
  - **exec** command
- SSL-Admin—Can administer all SSL features:
  - SSL—Create permission
  - PKI—Create permission
  - Interfaces—Modify permission
  - Copy configurations—Create permission
  - **changeto** command—Create permission
  - **exec** command

Configuring RBAC

To create a domain and a user, and associate the user with a predefined role and the new domain, you can use either the ACE Device Manager user interface (GUI) or the CLI.

- Configuring RBAC Using the Device Manager GUI
- Configuring RBAC Using the CLI

For more information on advanced virtualization configuration, such as restricting user access, predefined roles and how to define a custom role, and creating a domain, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

Configuring RBAC Using the Device Manager GUI

In this procedure, you use the GUI to create a domain that includes the user context that you created in Chapter 3, Creating a Virtual Context and then create a server maintenance user, user1, to manage those servers. Configure this RBAC setup using the GUI by following these steps:

Step 1 Choose **VC_web**.

Step 2 Choose **Admin > Role-Based Access Control > Domains**. The Domains pane appears.

Step 3 Click **Add (+)** to add a new domain. The New Domain window appears.

Step 4 Enter **Domain1** for the Name.

Step 5 Check the **All Objects** check box.

Step 6 Click **Deploy Now** to create a domain that includes all objects in context VC_web.

Step 7 Choose **Role-Based Access Control > Users** to create a user. The Users pane appears.

Step 8 Click **Add (+)**. The User window appears.

Step 9 Enter the following user attributes. Leave the remaining attributes blank or with the default values.

- Name: user1
- Password: MYPASSWORD
- Confirm: MYPASSWORD
- Role: Server-Maintenance

Step 10 Choose **Domain1** and click the **right-arrow** button. Domain1 is moved from Available to the Selected list.

Step 11 Choose **default-domain** and click the **left-arrow** button. Default-domain is removed from the Selected list.

Step 12 Associate the new user user1 with the role Server-Maintenance and the domain Domain1 by clicking **Deploy Now**. The new user is added to the Users pane.

Configuring RBAC Using the CLI

Configure RBAC using the CLI by following these steps:

Step 1 Verify that you are operating in the desired context by checking the CLI prompt. If necessary, change to the correct context.

```
host1/Admin# changeto VC_web
host1/VC_web#
```

Step 2 Enter configuration mode.

```
host1/VC_web# Config
host1/VC_web(config)#
```

Step 3 Create a domain for the context.

```
host1/VC_web(config)# domain Domain1
host1/VC_web(config-domain)#
```

Step 4 Allocate all objects in the VC_web context to the domain.

```
host1/VC_web(config-domain)# add-object all
host1/VC_web(config-domain)# exit
host1/VC_web(config)#
```

Step 5 Configure new user user1, and assign the predefined role TECHNICIAN and the domain Domain1 to the user.

```
host1/VC_web(config)# username user1 password 5 MYPASSWORD role TECHNICIAN domain Domain1
```

Note The parameter 5 for password is for an MD5-hashed strong encryption password. Use 0 for a clear text password.

```
host1/VC_web(config)# exit
```

Step 6 Display the user and domain configurations.

```
host1/VC_web# show running-config role
host1/VC_web# show running-config domain
```

Configuration Example for Configuring RBAC

The following example shows how to configure RBAC. The commands that you have configured in this chapter are shown in bold text.

```
switch/VC_web(config)# do show running config
Generating configuration....

access-list INBOUND line 8 extended permit ip any any

class-map type management match-any REMOTE_ACCESS
  description Remote access traffic match
  2 match protocol ssh any
  3 match protocol telnet any
  4 match protocol icmp any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
  class REMOTE_ACCESS
    permit

service-policy input REMOTE_MGMT_ALLOW_POLICY

interface vlan 400
  description Client connectivity on VLAN 400
  ip address 10.10.40.1 255.255.255.0
  access-group input INBOUND
  no shutdown
interface vlan 500
  description Server connectivity on VLAN 500
  ip address 10.10.50.1 255.255.255.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 172.25.91.1

domain DOMAIN1
add-object all
username USER1 password 5 $1$vAN9gQDI$MmbmjQgJPj45lxbtzXPpB1 role Server-Maintenance
domain DOMAIN1
```

Where to Go Next

In this chapter, you have created a user to perform a limited number of functions on a subset of your network. Next, you will create a virtual server for server load balancing.