CHAPTER 4

Controlling intra-site business access

This chapter discusses what can happen once a user is allowed VLAN access by the network access policy. In OverDrive, this is controlled by business access policies.

Install type: intra-site business policies

For intra-site access, an admin creates business policies that connect a VLAN to a local resource at the same site. You can further manage intra-site networks by concentrating on business policies as explained in this chapter.

Getting oriented

This chapter is based on a network pre-populated with a number of sites having devices such as Cisco switches, DSCs on OverDrive appliances, and various routers.

In the network status view, if we drill down to the Chicago site in the Central domain, and right-click the DSC, we can choose to see logs, graphs, or the active policy; or, we can choose to configure the DSC.

If you look at the DSC's log, you see tabs that let you choose a particular log: the DSC health, ntpd's success at synchronizing with the time server, and the results of the DSC's polling of the device (the DSC might be looking to see if there are any tunnels defined, for example).

If you go to the device itself (in this case, the router named CISCO1800-65134), you can execute device commands to show the device configuration, its interfaces, and its routes. For example, Show Configuration produces a device command log:

Since this is a Cisco device, the log reports a typical Cisco configuration coming up.

The device and DSC commands are configurable and can be added to and edited.

Building a primary network policy

This section walks you through building a primary network policy.

Notice in the following figure from the domain tree view that there are policies that are grayed out because they're not active yet.

We refer to these as different types of policies, shown here as access and network policies, but under the covers, they are really the same—these all happen to be business access policies. That is, they build associations between resources at one site and resources at another site. Or between resources on network switches on one site and other resources at that site.

Note OverDrive supplies a suggested naming scheme for objects that you create. For network access policies such as discussed in the previous chapter, OverDrive provides a pre-filled name prefix, **Network Access Policy:** (for business policies, the prefix is **Business Policy:**).

If you right-click a policy and choose Edit, you can see immediately whether it is a business or a network access policy. If you could do that for all the policies in the preceding figure, you would see that they are all business policies. Business policies determine what you are allowed to reach on the net, for instance, whether you can go to specific servers, and when. These policies provide the logic that allows you to do your business.

Editing and activating a primary networking policy

The primary networking policy described here constructs a connection between each of the subnets at different sites.

1. If you could, create a business policy named Network Policy: Primary Network, similar to the one shown in the following figure.
2. Place five site-specific subnets as participating resources in the pane on the right. One of them is the Boston primary data center. The other four (Chicago, Dallas, Nashville, and San Francisco) are to connect to Boston.

   This policy uses a hub and spoke configuration, with the Boston primary data center as the hub.

3. Open the Ports & Protocols tab and choose ANY as the protocol so any traffic can go through.
4. Click Submit.

   The status will still be inactive (as you can see in the upper right), because the policy has not yet been activated.

5. Activate the policy by right-clicking it in the domain tree and choosing Activate.
6. Notice that the gear becomes blue:

Verifying the policy

The NSVE now reconfigures the network. That is, it creates VPNs connecting, in this case, the four spoke sites to the central hub. This process is known as policy server provisioning, which means figuring out how to change all the sites that need to be changed to make the policy true.

The NSVE sends configuration directives to every site that has one of the participating resources, and builds connections back to the hub, using the DSCs at those sites.

In the business status view, these are the policies that have to be put into effect to make the policy true. Each of the devices responds to the DSC's poll asking the status of its connections. Once those connections are up, the devices report back to the DSCs, and the DSCs report back to the status view and say okay, the connections are up, the tunnels are in place, and communication is occurring over them.

Note The connections only show as green when there is traffic passing through them. Red doesn't indicate a connection is down, but rather that is shows no traffic.

If you mouse over, you get a tooltip that shows you the characteristics of the connection, for example, showing that the subnet at Boston is connected to the subnet at Chicago, and with which IP addresses, for instance.

Note In this example, there are only routers and no switches. These are just site interconnects.

Viewing the active policy

When the connections are all up:

1. Go back to the network status view, and pick one of the sites.

   For this example, choose the Boston data center (the hub).
2. Right-click the DSC and choose View Active Policy.
3. Look for a report such as the following (shown in part):

At the top are the four IPsec connections that were built to support the policy, including a description of the connections that had to be built. Below those are the subnet connections, followed by the firewall policy that reflects what is allowed across the connections, followed by VLAN connections (none, in this case).

Viewing device configurations

Now, view the device configuration:

1. In the network status view, right-click one of the Boston devices such as the distribution switch, and choose Execute Device Command > Show Configuration.
2. Look for the effects of the provisioning commands on the router, including static and dynamic routes, and ACLs.

And view the VLAN connections, including ID, name, IP address, subnet mask, inbound and outbound ACL settings, and ports.

Changing network topology

Suppose you need to allow the sites to communicate with each other.

You can change network topologies very easily. For example, you might prefer a full-mesh connection, instead of a hub-and-spoke. With a full-mesh connection, every site connects to all the others. With a hub-and-spoke, you have to go to each spoke site and build a connection from it to the hub.

Without OverDrive, it takes a lot of preparation and work for a network engineer to make this change without error.

With OverDrive, it's easy:

1. Right-click the business policy, e.g., Network Policy: Primary Network and choose Edit.
2. Click the configuration drop-down and choose Full Mesh.
3. Click Submit.

   OverDrive figures out what needs to change, or not, and decides what has to be added to current or new connections to satisfy the policy.
4. Check the business status view to be sure traffic flows between all the sites.

   For example, the status view in the following figure has a tooltip showing a problem: cannot provision:

   In this case, the router is not talking to the DSC. SeeTable 7-1 on page 7-3, which explains that the DSC on the left (for the Boston subnet) has not been deployed.
5. Finally, confirm that all connections are up and all green

Section summary

These steps have illustrated a basic inter-site connection policy connecting sites together. Anyone at any of the sites can access any of the resources on the other sites in this full-mesh network.

Creating a business policy for a CRM server

Consider a business policy that allows access to a CRM (customer relations management) server. Suppose you have sales people in a collection called Sales. These include all the people in an in-house sales force. When you build the policy, you don't care where the sales people are, or who they are individually. You need to give them all access to the CRM server.

To create the policy and activate it:

1. Create a new local resource named Server-VM: CRM in, for example, the San Francisco - Secondary Data Center.
2. Create a business policy called Business Policy: CRM Access, in a subdomain containing the San Francisco and Boston data centers.
   a. Assign a set of ports and protocols that are specific for the connection.

      The following figure shows an example of ports and protocols for an Exchange server, with certain TCP ports; you could possibly add certain UDP ports.

   b. Assign it resources such as PC: Dallas Accounting J101 and other sales-related resources as shown in the following figure. Also, assign the CRM server:

c. Choose hub and spoke for the configuration, as shown above, and select the CRM server as the hub.

d. Accept the default scheduler to start immediately, with no end date, or change it as you wish:

3. Click Submit.

   OverDrive activates the policy and gives it all the connections needed to satisfy it. The connections should come up quickly.

4. Check the connections in the business status view.

You might see that neither side of a connection comes up, as in the figure below, where the green icons and tooltip signify that the DSCs are up, but haven't yet confirmed a connection between them to support this policy.

To troubleshoot the connections, you might:

1. Find the DSC in the network status view.
2. Right-click the DSC, and choose View Log.
3. See if the DSC thinks the connection is down for some reason.

You have to be quick, because the connection might come up while you're looking at the log, as it has below: