CHAPTER 5

Data Center/Campus Service Module Design Considerations

Enterprise customers often handle the day-to-day operations and management of building system networks. In terms of the energy management solution, the function of the Data Center/Campus Service Module is to provide a centralized point of administration and operations, referred to as an Energy Management Operations Center (EMOC) within this document. This allows the enterprise organization to centrally manage the Mediators deployed both within the campus as well as within the branches. The components of the energy management solution that may reside within the EMOC are as follows:

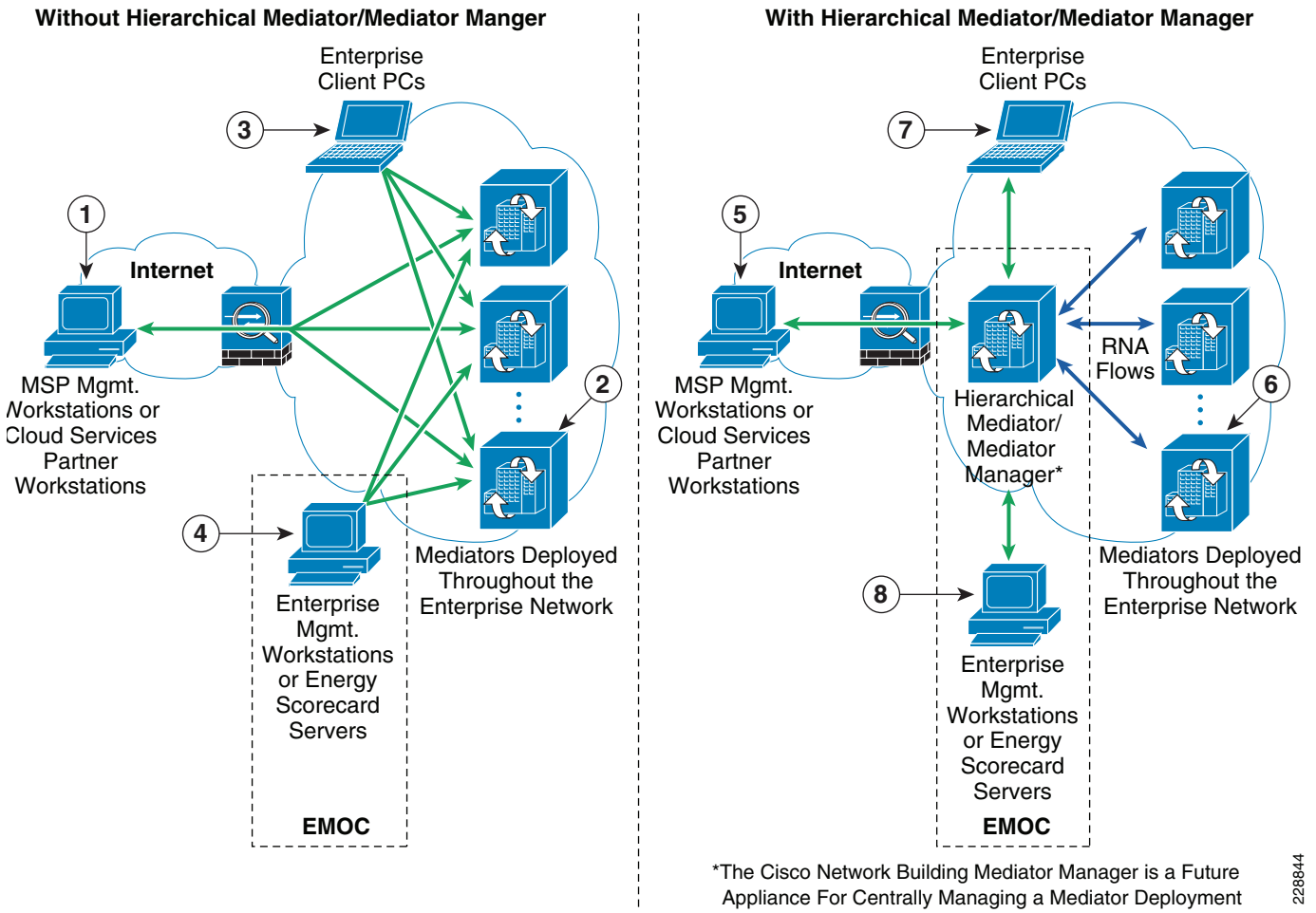
- *Enterprise Energy Management Workstations*—These provide the ability to configure the Mediators via the configTOOL management application; to create and deploy graphical-based logical control applications to the Mediators via the perfectHOST application; and to monitor and manage aspects of the Mediators such as set points, events and alarms, and websites created and deployed on the Mediators, via the OMEGA suite of applications.
- *Enterprise Archiving and Energy Scorecard Servers*—These optional servers may be deployed in order to collect and archive periodically exported datapoint information from the Mediators. This information may then be used to provide an internal energy scorecard and/or historical energy usage information for both energy management personnel and business units within the enterprise organization. In business scenarios where the enterprise organization has outsourced this function to a cloud service provider, these servers may not be deployed. Note also that separate servers may be used for the datapoint archiving function and the energy scorecard function.
- *Hierarchical Mediator/Mediator Manager*—The hierarchical Mediator is an optional component which provides the ability to centrally collect and display datapoints on remote Mediators via the use of aliases and the Remote Node Abstraction (RNA) protocol. Note that any Mediator can share datapoint information with another mediator in a peer-to-peer manner. The hierarchical Mediator design is simply a design option in which one or more Mediators functions as an aggregation point for downstream Mediators. The Cisco Network Building Mediator Manager (Mediator Manager) is a future product offering, which will scale the overall energy management solution deployment by offloading the hierarchical Mediator function to a server appliance.

Note This revision of the design guide focuses primarily on hierarchical Mediator designs. Future revisions will include further discussion of the Cisco Network Building Mediator Manager.

Hierarchical Mediator Designs

A hierarchical Mediator design allows datapoints from building devices connected to remote Mediators to be defined using aliases on a hierarchical Mediator centrally located. The Mediators use the Remote Node Abstraction (RNA) protocol to share datapoint information between themselves. To the hierarchical Mediator, the datapoints appear as if they were coming from devices directly attached to it. The hierarchical mediator model is designed to provide a single point of access, via websites deployed on the hierarchical mediator, to the datapoints for the Mediators deployed within the enterprise organization; versus having to access each Mediator individually. An example of this is shown in Figure 5-1.

Figure 5-1 Mediator Access With and Without Hierarchical Mediator Functionality



The following describes the numbers in Figure 5-1:

Without Hierarchical Mediator

- **1**—Managed service provider workstations need access to each Mediator in order to monitor and manage the deployment.

- **2**—Mediators individually export periodically logged datapoint information to cloud-services partner servers and/or enterprise energy scorecard servers. Event data may be exported by each Mediator individually, viewed and acknowledged on each Mediator individually, or viewed and acknowledged centrally on one Mediator through a cloud formation.
- **3**—Individual client PCs may need access to individual Mediators deployed throughout the enterprise organization, in order to view collected datapoint information via websites created and deployed on the Mediators.
- **4**—Enterprise energy management workstations need access to each Mediator in order to monitor and manage the deployment.

With Hierarchical Mediator

- **5**—Managed service provider workstations may need access to the hierarchical Mediator in order to view datapoint information (aggregated from remote Mediators through the RNA protocol) within websites deployed on the hierarchical Mediator. Depending on management requirements, individual access to each Mediator may still be required.
- **6**—Mediators individually export periodically logged datapoint information to cloud-services partner servers and/or enterprise energy scorecard servers. Event data may be exported by each Mediator individually, viewed and acknowledged on each Mediator individually, or viewed and acknowledged centrally on the hierarchical Mediator through a cloud formation.
- **7**—Individual enterprise client PCs may need access to the hierarchical Mediator in order to view datapoint information within websites created and deployed on the hierarchical Mediator.
- **8**—Enterprise energy management workstations may need access to the hierarchical Mediator in order to view datapoint information within websites deployed on the hierarchical Mediator. Depending upon management requirements, individual access to each Mediator may still be required.

One advantage of implementing hierarchical Mediator functionality is that it may be possible to restrict enterprise client PCs which need access to energy management information directly from the Mediators, to only the hierarchical Mediator. This has security advantages in terms of configuration of access control and monitoring to a single Mediator; versus allowing enterprise client PCs potentially spread throughout the network to access individual Mediators. It may also be possible to restrict MSP partner VPN access to only the hierarchical Mediator device deployed within the EMOC - depending upon the management requirements. Note however that current hierarchical Mediator functionality requires RNA functionality to be configured on both the hierarchical Mediator and remote Mediators. This requires initial management workstation access to both. Further, ongoing changes to the configuration of the Mediators through the configTOOL, and/or applications deployed on the Mediators via perfectHOST; may still require the MSP partner management servers and enterprise management servers to have direct access to the remote Mediators.

The current hierarchical Mediator functionality allows for the datapoints on remote Mediators to be aliased, so that they appear to be local datapoints on the hierarchical mediator, and are automatically collected from the remote Mediators via the RNA protocol. Websites created on the hierarchical Mediator can then display datapoint information on the remote Mediators as if it were local to the hierarchical Mediator. Note that the current hierarchical Mediator design has scale limitations which depend on factors such the number of remote Mediators deployed, the number of datapoints aliased from those remote Mediators, the collection interval of the datapoints, and the number websites deployed and accessed on the hierarchical Mediator. The Cisco Network Building Mediator Manager functionality is a future function targeted to be deployed on a dedicated server appliance, as opposed to a Mediator platform, to address such scalability concerns. It is targeted to scale to approximately 200 remote Mediators.

The following sections discuss the deployment of the Energy Management Operations Center (EMOC) as a service module within a larger data center design; as well as within a service module hanging off the campus core. The designs further discuss deployments in which VRFs have been used (using the VRF-Lite with GRE tunnel method) in order to provide path isolation of the energy management solution from the rest of the enterprise network; as well as non-VRF deployments.

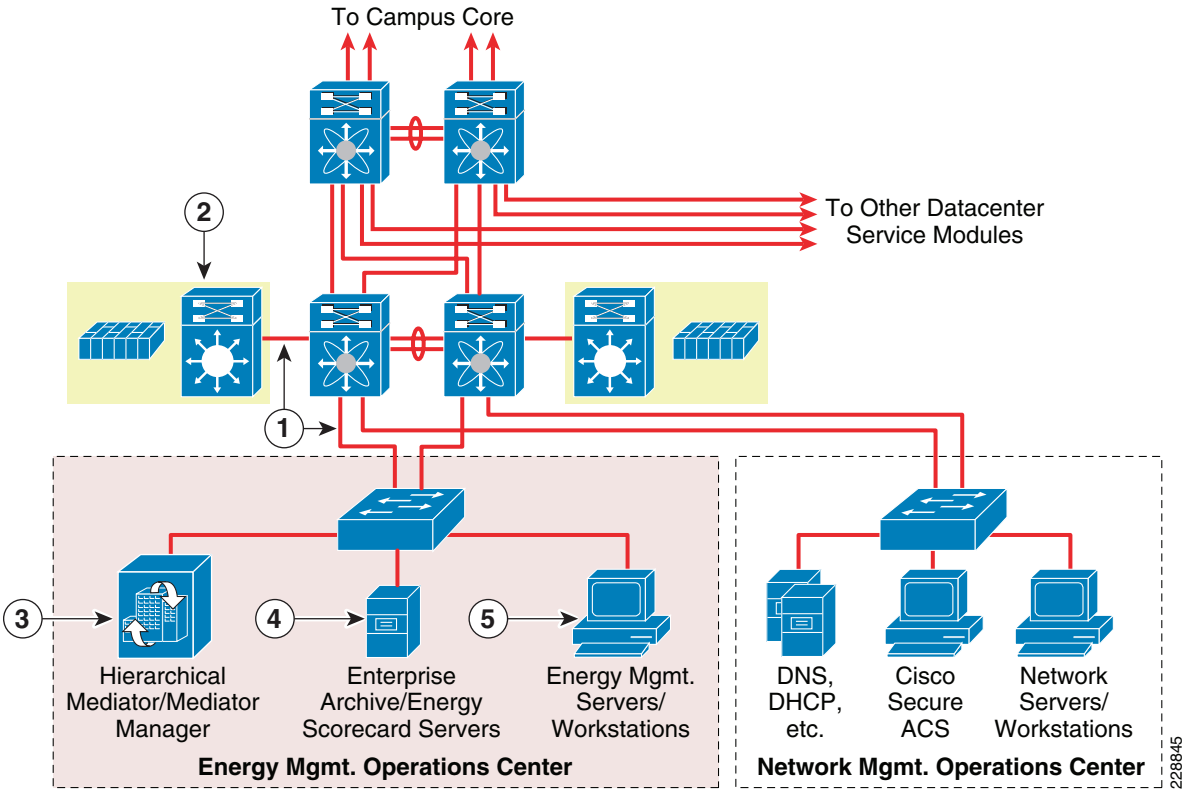
Data Center Service Module Design

In some situations, the facilities management personnel who are managing the energy management solution are physically located within a data center of the campus. In these scenarios, a separate service module hanging off of the overall data center design can be implemented for the EMOC. The following sections discuss data center EMOC designs from both a non-VRF and VRF perspective.

Non-VRF Designs

Figure 5-2 shows an example of a Data Center Service Module design without the use of VRFs.

Figure 5-2 Non-VRF Data Center Service Module Design with Catalyst 6500 Service Switch and FWSM



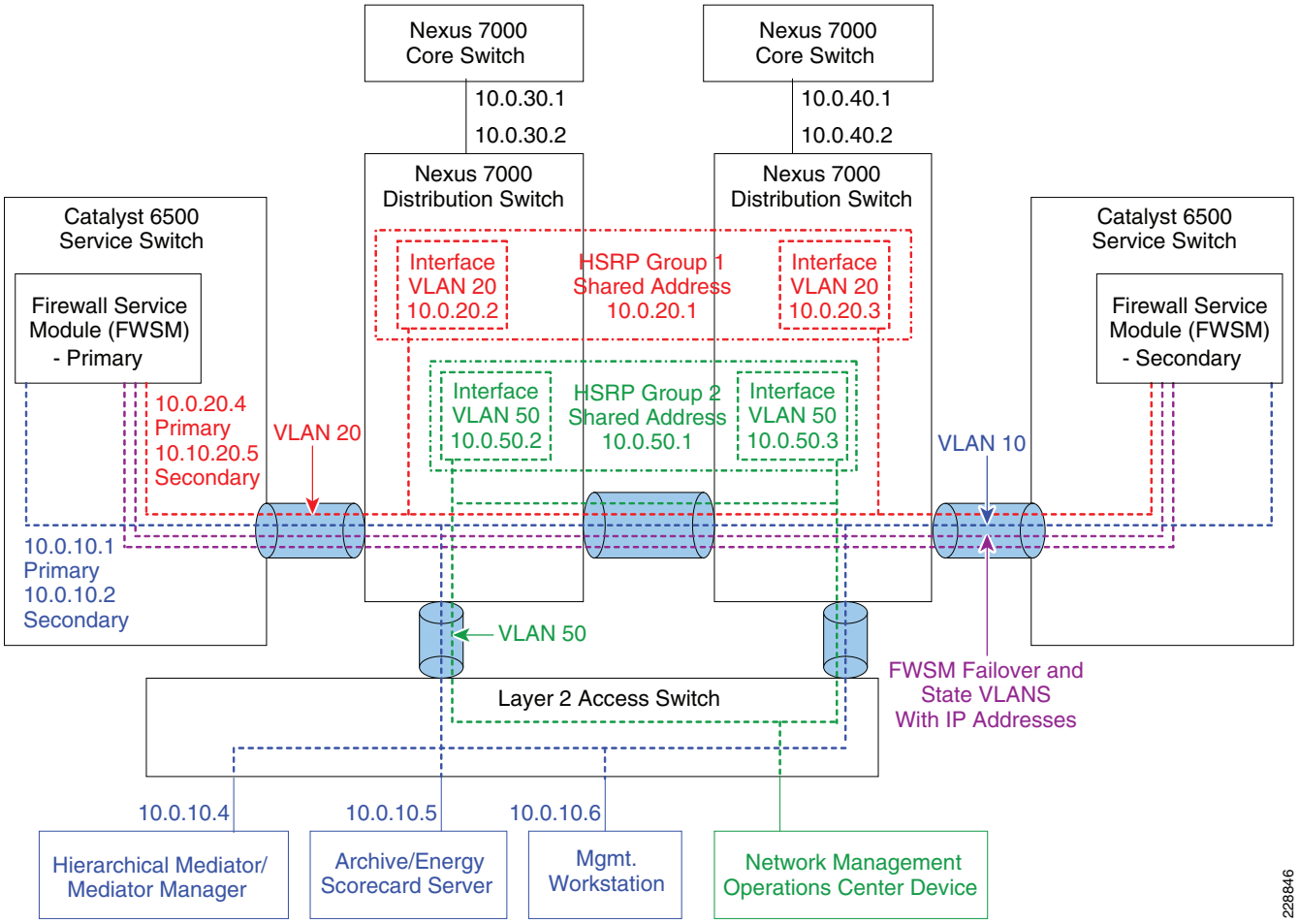
The following describes the numbers in Figure 5-2:

- **1**—Energy Management Operations Center (EMOC) VLAN trunked through Nexus 7000 Distribution Switch and the Catalyst 6500 Service Switch to the FWSM.
- **2**—FWSM in the Catalyst 6500 Service Switch provides stateful access control to and from the EMOC devices.

- **3**—Hierarchical Mediator functionality can provide a real-time single point of access to energy usage information (datapoints) from Mediators deployed throughout the enterprise network.
- **4**—Internal enterprise archive servers may collect periodically exported datapoint information from individual Mediators deployed throughout the network infrastructure. An energy scorecard service may make historical energy usage information available internally within the organization.
- **5**—Internal enterprise management workstations may be used to configure the hierarchical and/or remote Mediators; deploy logical control applications to the hierarchical and/or remote Mediators; and to create, monitor, and deploy websites to the hierarchical and/or remote Mediators.

In this example, a separate EMOC VLAN is implemented within the Data Center Service Module. The EMOC VLAN is trunked from the access switch, through the Nexus 7000 Series data center Distribution Switch, to a Layer-3 interface of the FWSM module located within the Catalyst 6500 Service Switch. The FWSM then provides stateful access control to and from the EMOC VLAN. A more detailed example is shown in Figure 5-3.

Figure 5-3 Detailed Example of Data Center Service Module Design with Catalyst 6500 Service Switch and FWSM



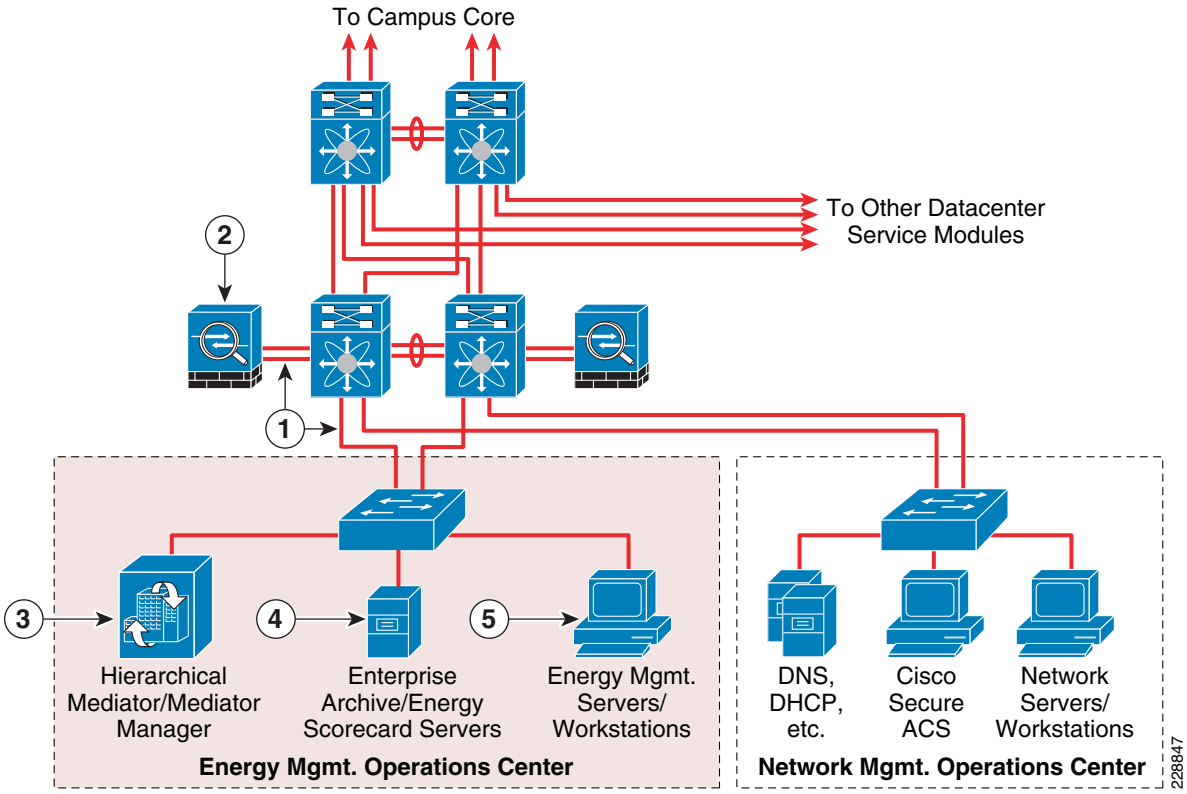
Note that there are many different ways in which firewalling of the EMOC VLAN could be achieved within the data center, because the FWSM supports both transparent (Layer 2) and routed mode (Layer 3) firewalling, high-availability through active/active or active/standby firewall configurations, and single or multiple context (virtual firewalls) mode. This example shows only one highly simplified method using a single context, routed mode firewall in an active/standby configuration. IP addressing

has been arbitrarily chosen for example purposes only. In this configuration, when the primary FWSM fails, the secondary FWSM takes over its IP and MAC addresses. From the perspective of the EMOC devices nothing has changed. However, traffic flows to the secondary FWSM located within the second Catalyst 6500 Service Switch. Stateful firewalling is done on the FWSM between VLANs 10 and 20 in the example, corresponding to IP subnets 10.0.10.0 and 10.0.20.0.

Other VLANs such as a Network Operations Center (NOC) VLAN can also be supported off the same Data Center Service Module, as shown in Figure 5-2 and Figure 5-3. The NOC VLAN can support traditional functionality such as network management servers, DNS, and DHCP, as well as the Cisco Secure Access Control Server which provides AAA services for MSP Partner VPN access to the enterprise network. For example purposes only, the design shows traffic from the Network Management Operations Center (NMOC) VLAN not passing through the FWSM. In actual deployments, this may be firewalled as well.

An alternative to the Catalyst 6500 Service Switch with FWSM design is to implement a set of ASA 5500 Security Appliances within the Data Center Service Module, as shown in Figure 5-4.

Figure 5-4 Data Center Service Module Design with ASA 5500 Security Appliances



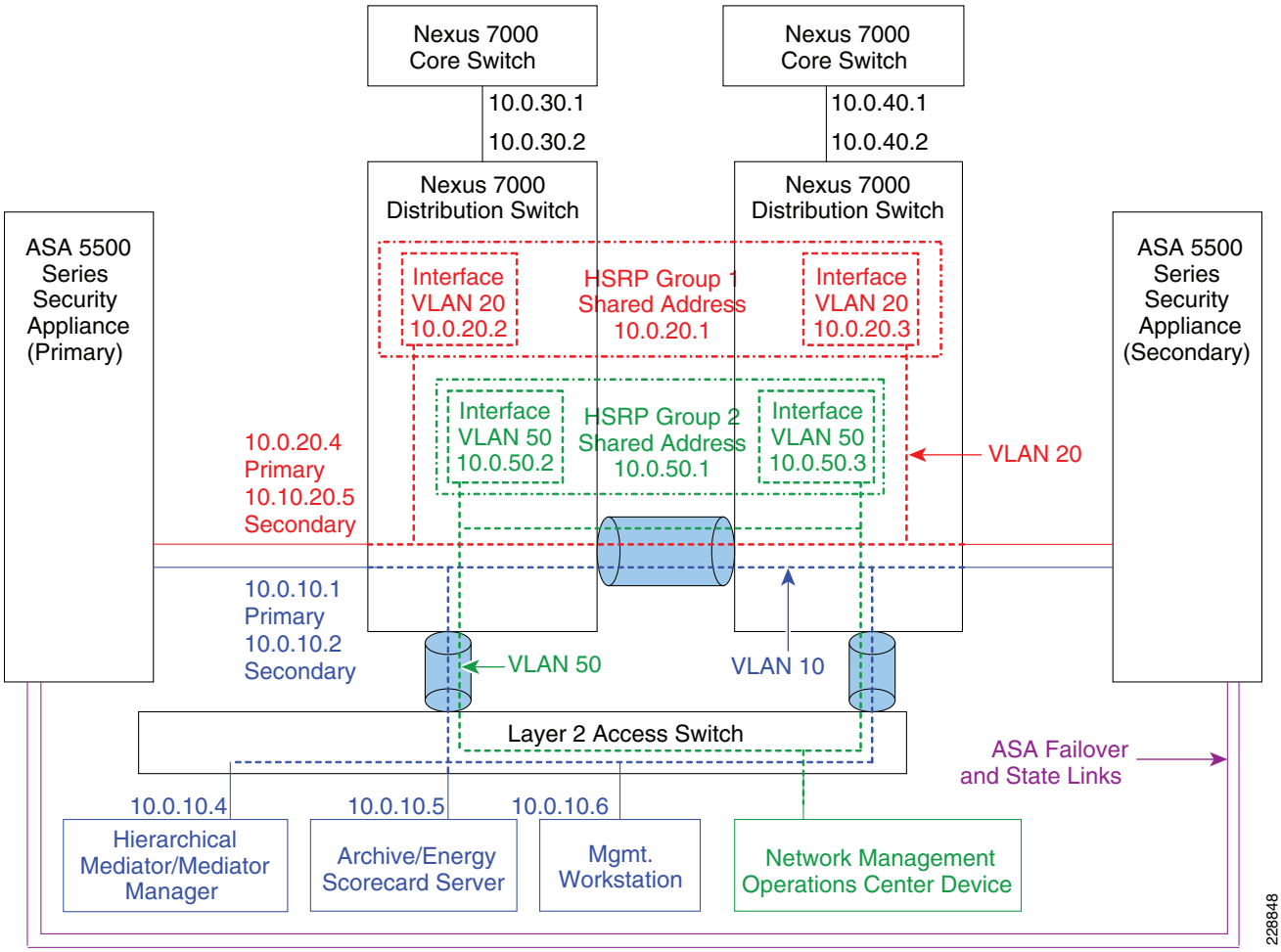
The following describes the numbers in Figure 5-4:

- **1**—EMOC VLAN trunked through Nexus 7000 Distribution Switch to ASA 5500 Security Appliances.
- **2**—ASA 5500 Security Appliances in the data center provide stateful access control to and from the EMOC devices.
- **3**—Hierarchical Mediator functionality can provide a real-time single point of access to energy usage information (datapoints) from Mediators deployed throughout the enterprise network.

- **4**—Internal enterprise archive servers may collect periodically exported datapoint information from individual Mediators deployed throughout the network infrastructure. An energy scorecard service may make historical energy usage information available internally within the organization.
- **5**—Internal enterprise management workstations may be used to configure the hierarchical and/or remote Mediators; deploy logical control applications to the hierarchical and/or remote Mediators; and to create, monitor, and deploy websites to the hierarchical and/or remote Mediators.

In this design, the EMOC VLAN is again trunked from the access switch, through the Nexus 7000 Series data center Distribution Switch, to a Layer-3 interface of the ASA 5500 Series Security Appliance. The ASA 5500 provides stateful access control to and from the EMOC VLAN. A more detailed example is shown in Figure 5-5.

Figure 5-5 Detailed Example Data Center Service Module Design with ASA 5500 Series Security Appliances



Again, note that there are many different ways in which firewalling of the EMOC VLAN could be achieved within the data center, because the ASA 5500 Series supports both transparent (Layer 2) and routed mode (Layer 3) firewalling, high-availability through active/active or active/standby firewall configurations, and single or multiple context (virtual firewalls) mode. This example shows only one highly simplified method using a single context, routed mode firewall in an active/standby configuration. IP addressing has been arbitrarily chosen for example purposes only. Individual interfaces are shown in this example, although VLAN sub-interfaces could also be used. In this configuration, if the primary ASA 5500 fails, the secondary ASA 5500 takes over its IP and MAC addresses. Again, from the

perspective of the EMOC devices nothing has changed. However, traffic flows to the secondary ASA 5500. Stateful firewalling is done on the ASA 5500 between VLANs 10 and 20 in the example, corresponding to IP subnets 10.0.10.0 and 10.0.20.0.

Since the examples in Figure 5-2 and Figure 5-4 4 do not assume a separate VRF for the Energy Management Solution, access control into the EMOC VLAN should be very tightly controlled. Figure 5-6, Figure 5-7, and Figure 5-8 show the protocols which may be allowed through the firewall.

Figure 5-6 Inbound Management and Monitoring Flows From MSP Partner

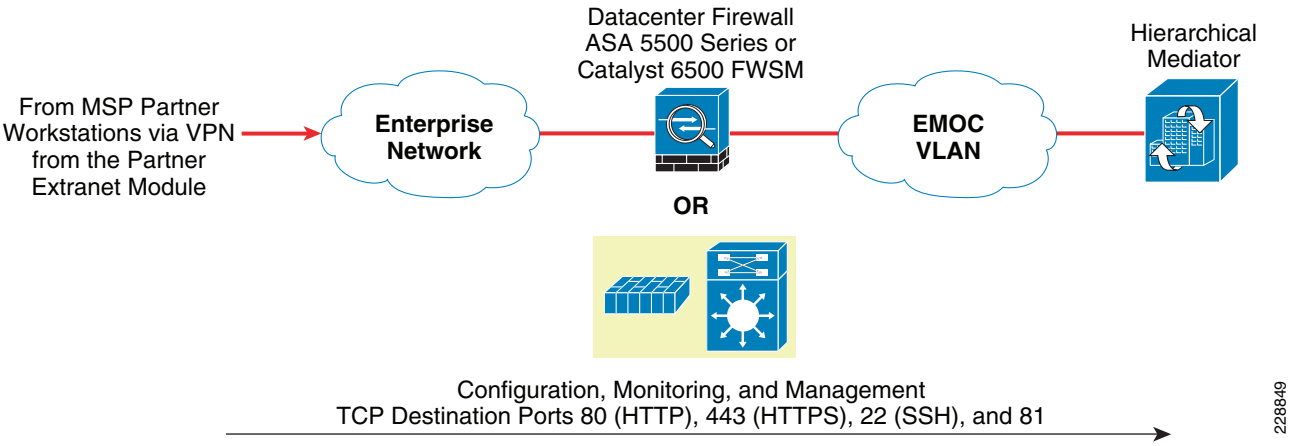
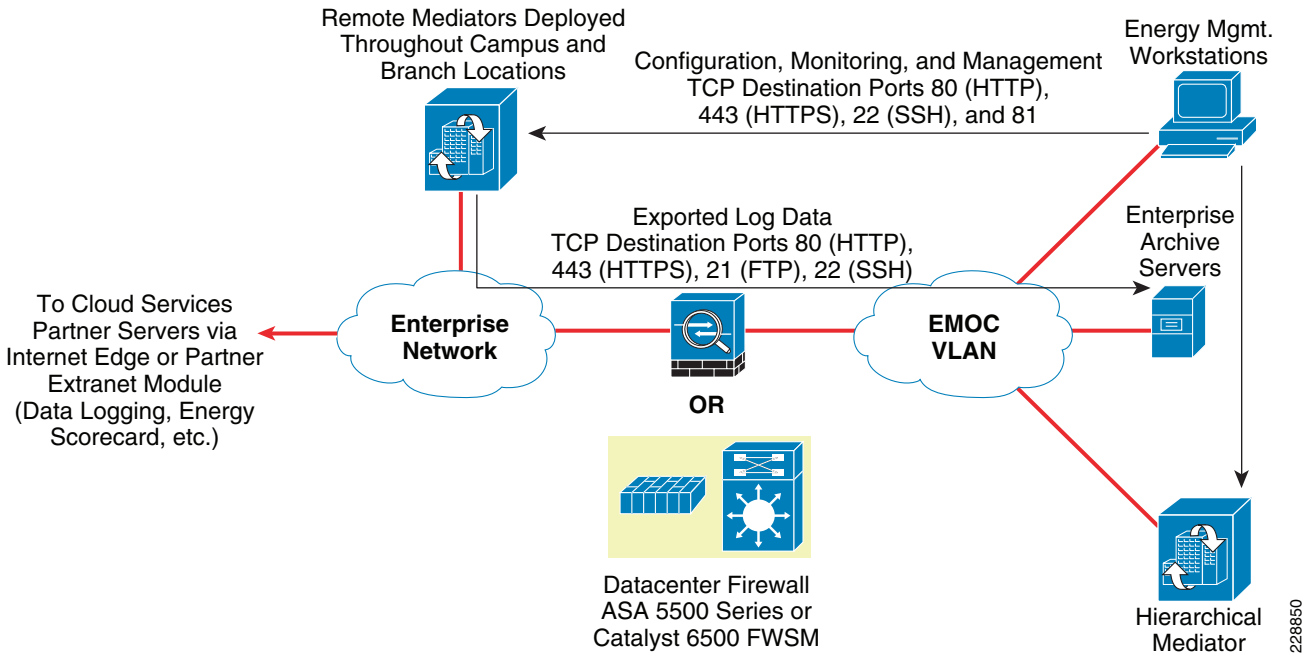


Figure 5-6 shows an example in which a MSP partner is providing management and/or monitoring of the Mediator deployment through a hierarchical Mediator deployed within the EMOC. In such cases, HTTP (TCP port 80), HTTPS (TCP port 443), SSH (TCP port 22) and TCP port 81 protocols need to be allowed inbound from the campus network through the data center firewall to the hierarchical Mediator within the EMOC. These allow inbound connectivity for the configTOOL, perfectHOST, and OMEGA suite of applications. The access control should be specified down to the IP address or addresses of the individual MSP partner workstations which connect to the enterprise network via either remote-access VPN or site-to-site VPN at the Partner Extranet Module. Note that the MSP partner workstations may still need access to each individual Mediator, but this access does not pass through the data center firewall in this design.

Figure 5-7 shows an example in which remote Mediators deployed throughout the IP network infrastructure periodically export datapoint information to an enterprise archiving server located within the EMOC. The remote Mediators may simultaneously export to a cloud services partner reachable via the Internet as well, but the flows do not pass through the data center firewall and are therefore not shown in Figure 5-7.

Figure 5-7 Inbound Exported Datapoint and Outbound Management Flows



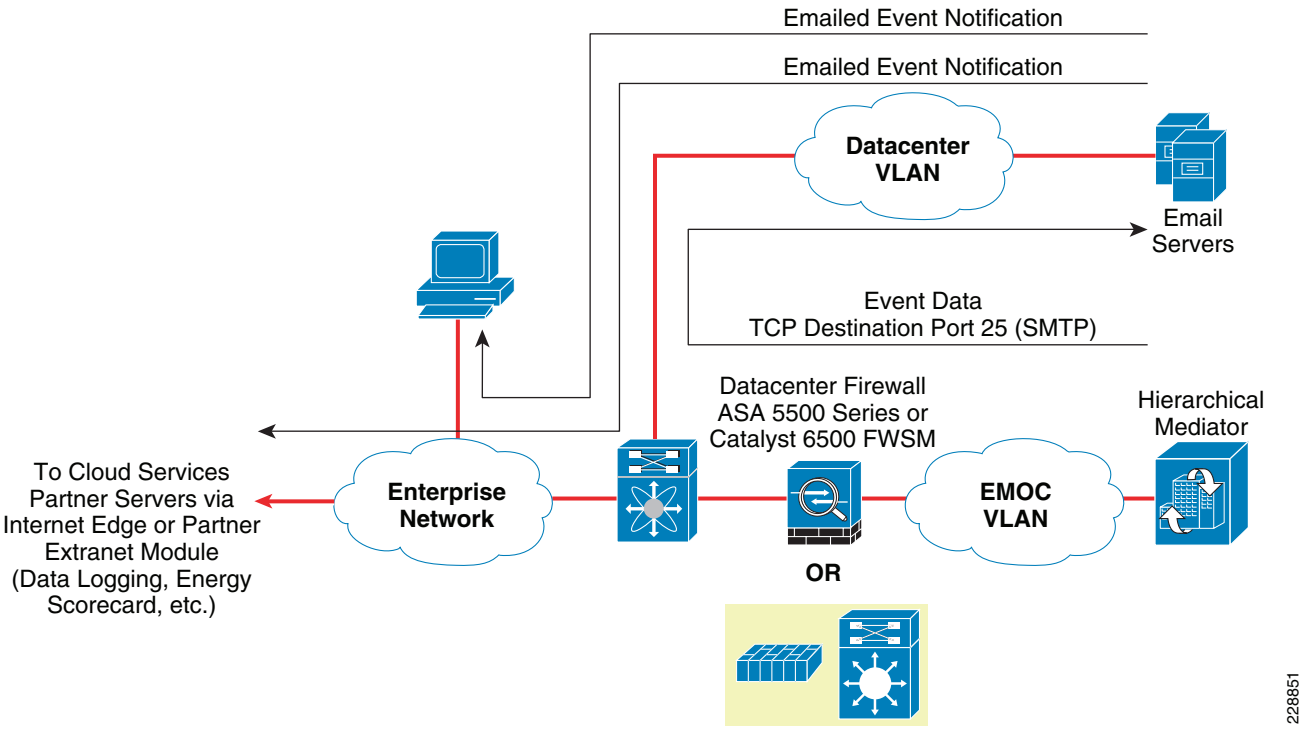
In such deployments, HTTP (TCP port 80), HTTPS (TCP port 443), FTP (TCP port 23), and/or SFTP that uses SSH (TCP port 22) needs to be allowed inbound from the remote Mediators through the data center firewall. Return traffic will automatically be allowed with a stateful firewall. In typical deployments, only a single protocol is used for the periodic exports. Note that when using FTP for periodic exporting of datapoint information, application-layer inspection of the FTP traffic is needed in order to dynamically open the data channel for the transport. Otherwise, a static range of ports may need to be opened for the data channel with FTP.

The enterprise energy management workstations also requires access each remote Mediator for configuration; deployment of graphical control applications; and the creation, deployment, and monitoring of websites on the remote Mediators. Therefore, HTTP, HTTPS, SSH, and TCP port 81 sessions initiated from the enterprise management workstations may need to be allowed from the EMOC out to the enterprise network, as is shown in Figure 5-7. No modifications to the data center firewall are needed for the enterprise management workstations to manage and monitor the hierarchical Mediator via the configTOOL, perfectHOST, and OMEGA suite of applications, provided the hierarchical Mediator is on the same VLAN segment as the enterprise management workstations.

Firewall access control should be specified down to the source IP address of the remote Mediator to the addresses of the enterprise archiving servers which receive exported datapoint information. Likewise, firewall access control should be specified down to the source IP address of the enterprise energy management workstation to the addresses of the individual Mediators deployed in branch and campus locations.

In some deployments it may be necessary for the hierarchical Mediator itself to export event data via the SMTP protocol through a corporate E-mail server. Figure 5-8 shows an example of this.

Figure 5-8 Exported Event Data via SMTP



For event data, Mediators deployed throughout the network can be configured to form a cloud. Event data can be viewed and cleared on any of the Mediators. If events are exported, each Mediator can export via the SMTP protocol (TCP port 25) to an E-mail server (or RSS server). Since the hierarchical Mediator may sit within the EMOC, SMTP traffic initiated by it must be allowed outbound through the data center firewall to the corporate E-mail servers that may reside on another data center VLAN segment, possibly hanging off another Data Center Service Module. In this example, the corporate E-mail server then forwards the event information to E-mail clients on enterprise client PCs as well as possibly MSP partner E-mail addresses or E-mail aliases.

Figure 5-9 RNA Flows Between Mediators

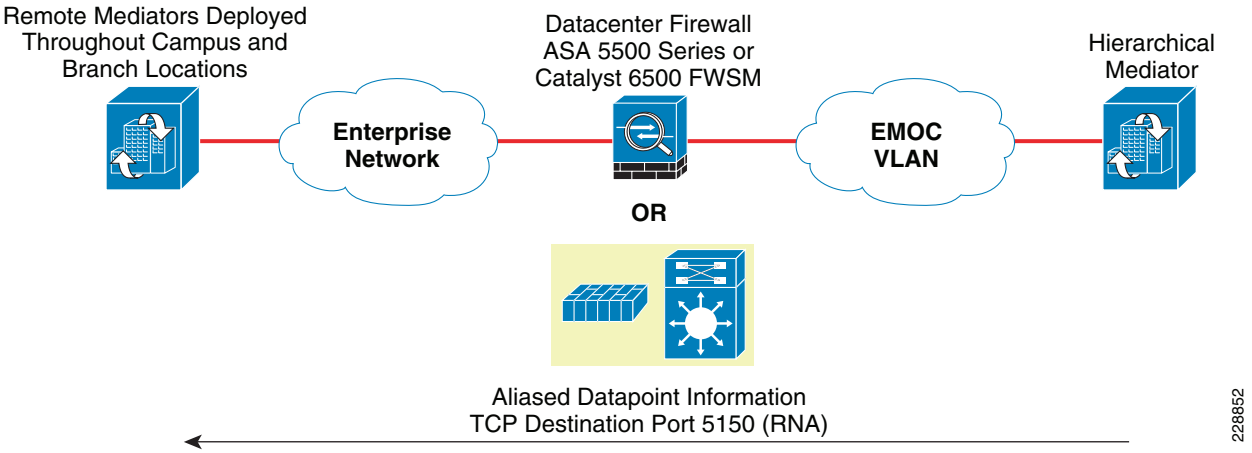


Figure 5-9 shows RNA flows (TCP port 5150) which need to be allowed outbound through the data center firewall in order for the hierarchical Mediator to automatically collect aliased datapoint information from remote Mediators deployed throughout the enterprise network. Note that in this example the hierarchical Mediator initiates the RNA flow, since the actual datapoints exist on the remote Mediators, and are aliased on the hierarchical Mediator. Access control should be specified down to the IP addresses of the individual Mediators in which datapoint information is being shared via the RNA protocol.

Figure 5-10 Data Center Flows with a Non-Hierarchical Mediator Design

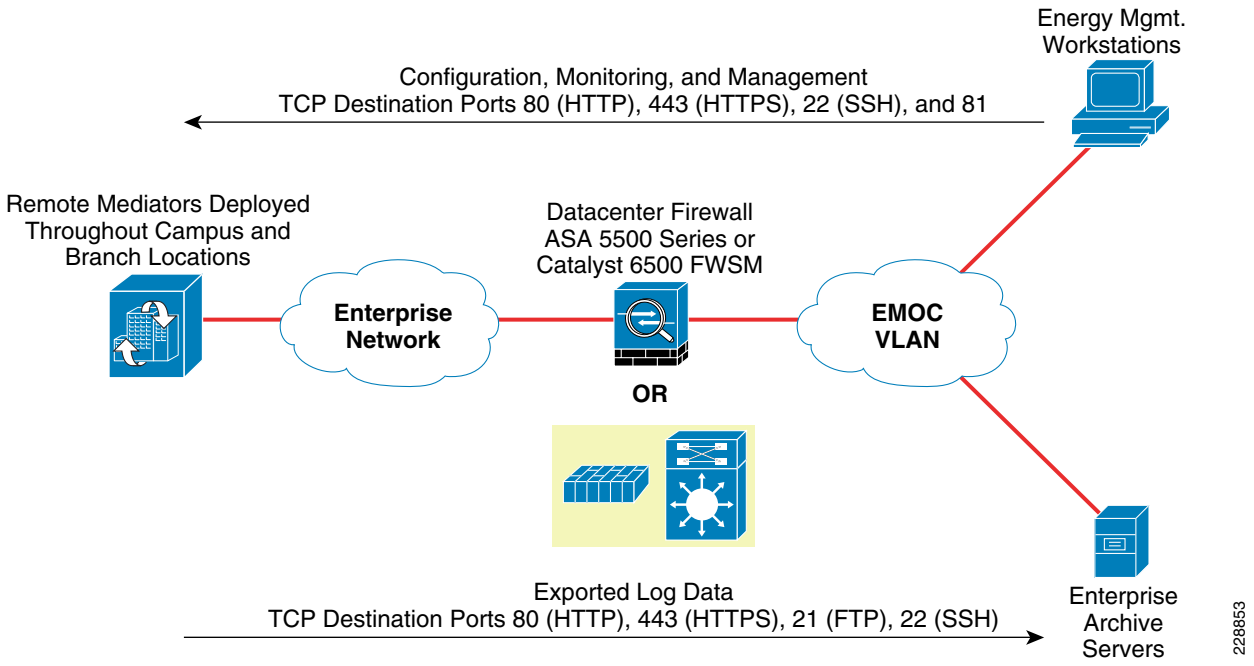


Figure 5-10 shows an example in which a hierarchical Mediator design is not deployed. In this model, the MSP partner servers individually access the Mediators deployed within the campus and branch locations. Therefore, MSP partner access into the EMOC may not be needed at all, and is therefore not shown in the figure. Sessions initiated from enterprise energy management servers located within the EMOC will still need to be allowed through the data center firewall to manage and monitor individual Mediators. Likewise, periodically exported datapoint information from each Mediator to the cloud services partner servers will not cross into the EMOC, and therefore do not need to be allowed through the data center firewall. However, periodically exported datapoint information from each Mediator to the enterprise archiving server will need to be allowed inbound through the data center firewall.

Enterprise Client PC Access to the EMOC

In some scenarios, business requirements include the need for client PCs sitting on the enterprise data network to access energy usage data. Access to energy usage data can be accomplished in the following ways:

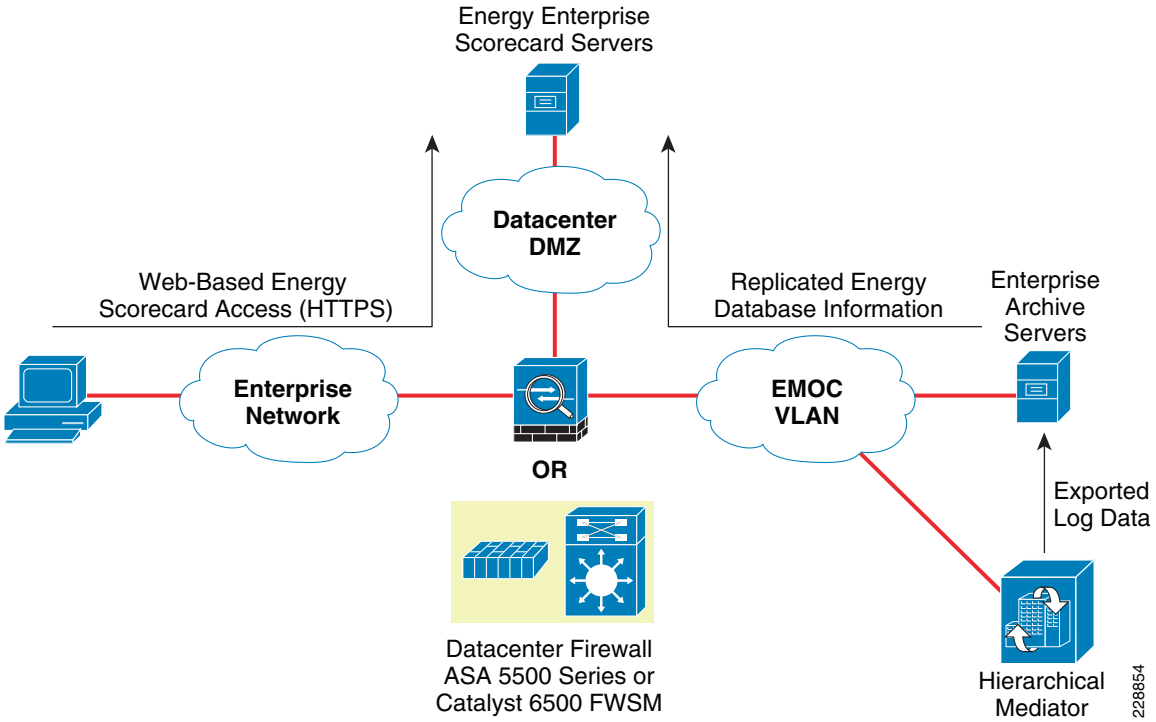
1. Client PCs access an energy scorecard website provided by a cloud services partner via the Internet.
2. Client PCs access an energy scorecard website provided internally by a partner or developed internally.

3. Client PCs directly access one or more websites deployed on the hierarchical Mediator which provides energy usage information.
4. Client PCs directly access websites deployed on Mediators deployed in branch and campus locations throughout the network infrastructure.

The first option is discussed in Chapter 4, "Internet Edge Design Considerations." This chapter discusses options 2 and 3. Option 4 is discussed within both Chapter 3, "Campus Design Considerations" and Chapter 6, "Branch Design Considerations."

When deploying an internal energy scorecard server, it may be beneficial from a security standpoint to separate the archiving function which collects and stores the periodically exported datapoint information from the Mediators, from the actual web/application server interface that client PCs access. This could be accomplished by implementing two servers: an energy scorecard web/application sever and an archiving server. One method of implementation is to have the energy scorecard web/application server remotely access a SQL database on the archiving server. Alternatively, and perhaps a bit more secure, would be to replicate the database information from the archiving server to the server which provides the web/application server interface for the energy scorecard. The energy scorecard server could then sit on a DMZ segment between the EMOC VLAN and the rest of the enterprise data network. Figure 5-11 shows an example of this type of design.

Figure 5-11 Example Client PC Access to Internal Energy Scorecard

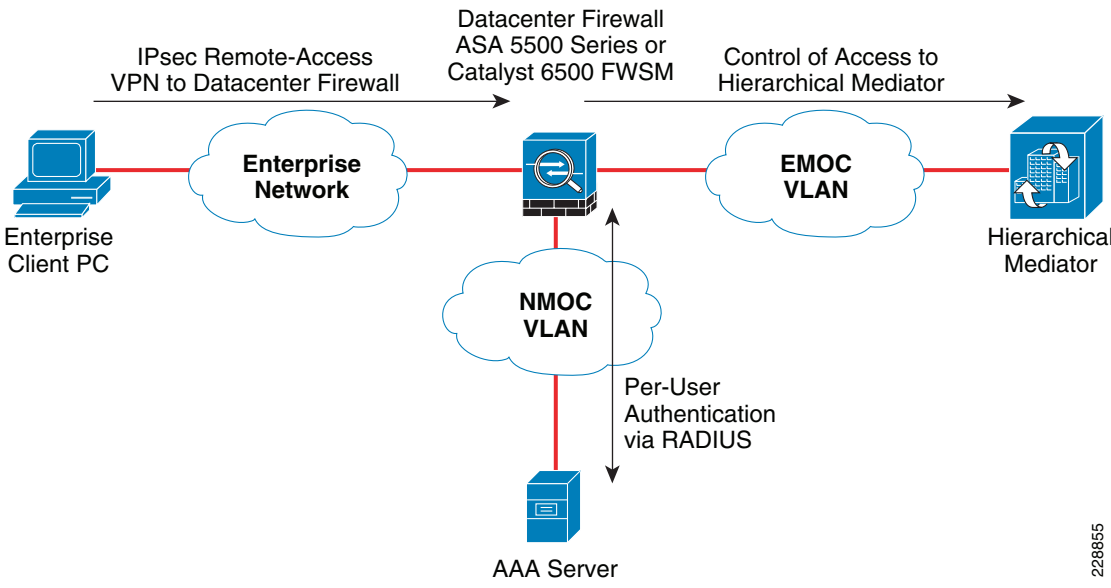


In this design, client PCs would be allowed to access only the energy scorecard server and not the actual Mediators which may be running logical control applications for building devices, or the actual archiving server which holds the historical database of logged datapoints. This continues to isolate the energy management solution from the rest of the data network, while still providing energy usage information to internal business units within the enterprise organization. The downside to this approach is that the

data may not be as “real-time” since the datapoint information is periodically exported and then replicated from the archiving server to the energy scorecard server; as opposed to directly accessing a Mediator via a website deployed directly on it.

Direct client PC access to websites deployed on the hierarchical Mediator within the EMOC is considered less secure than accessing an energy scorecard, yet still a somewhat more secure approach than allowing direct access to each remote Mediator. The hierarchical Mediator may be a dedicated device, configured only to collect aliased datapoint information from remote Mediators and display the information in custom websites developed for various internal business units within the enterprise organization; as opposed to directly interfacing with actual building systems. This approach requires direct inbound access from client PCs to the hierarchical Mediator within the EMOC; and therefore poses a higher security risk than accessing an energy scorecard. If business needs require enterprise client PCs to manage set points on the Mediators, rather than passively view datapoint information, direct access to the hierarchical Mediator may also be necessary. Where possible the use of HTTPS to access the hierarchical Mediator should be utilized. Userids and passwords on the hierarchical Mediator, restricting the particular website screens to the relevant business unit personnel, should be configured where possible. If possible, the access control from the data network to the EMOC should be restricted to a set of IP addresses which can only reach the hierarchical Mediator via the HTTPS protocol. For additional security the network administrator should consider two additional measures. First, the hierarchical Mediator itself may be placed on a DMZ segment off the data center firewall, between the enterprise client PC network and the EMOC. This is a similar design as was shown in Figure 5-11above. Client PCs would be allowed to access the hierarchical Mediator through the data center firewall via the HTTPS protocol. The hierarchical Mediator would be allowed to access the remote Mediators throughout the network via the RNA protocol. Alternatively, a second design is the deployment of IPSec remote access VPN on an ASA 5500 data center firewall. This would allow for access into the EMOC based on individual userid and password which can be controlled centrally via a AAA server. Figure 5-12 shows an example of this type of configuration.

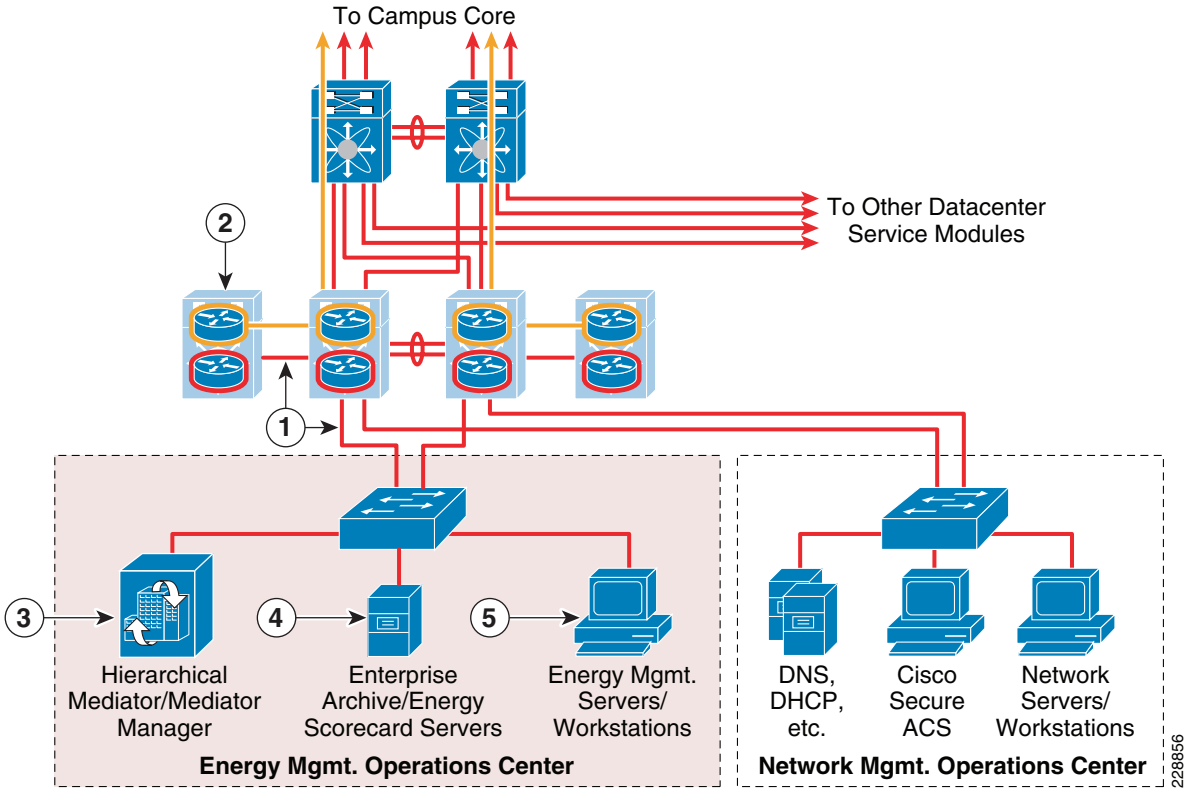
Figure 5-12 Example Client PC Access to Hierarchical Mediator



VRF Designs

The deployment of a separate virtual routing and forwarding instance (VRF) has the advantage of providing path isolation for the energy management solution. Since a separate energy management VRF already effectively isolates the traffic from the rest of the data, voice, and video traffic on the global VRF, stateful firewalling is not necessarily needed within the Campus Building Modules or within the branches. This means that controlling access between the energy management solution and the normal data network can be limited to one or more strategic points, versus being individually controlled within each campus building and each branch location. Figure 5-13 shows an example of a data center service module which makes use of VRFs to isolate the EMOC to a separate energy management VRF called the Building Infrastructure Network (BIN) VRF.

Figure 5-13 VRF Data Center Service Module Design



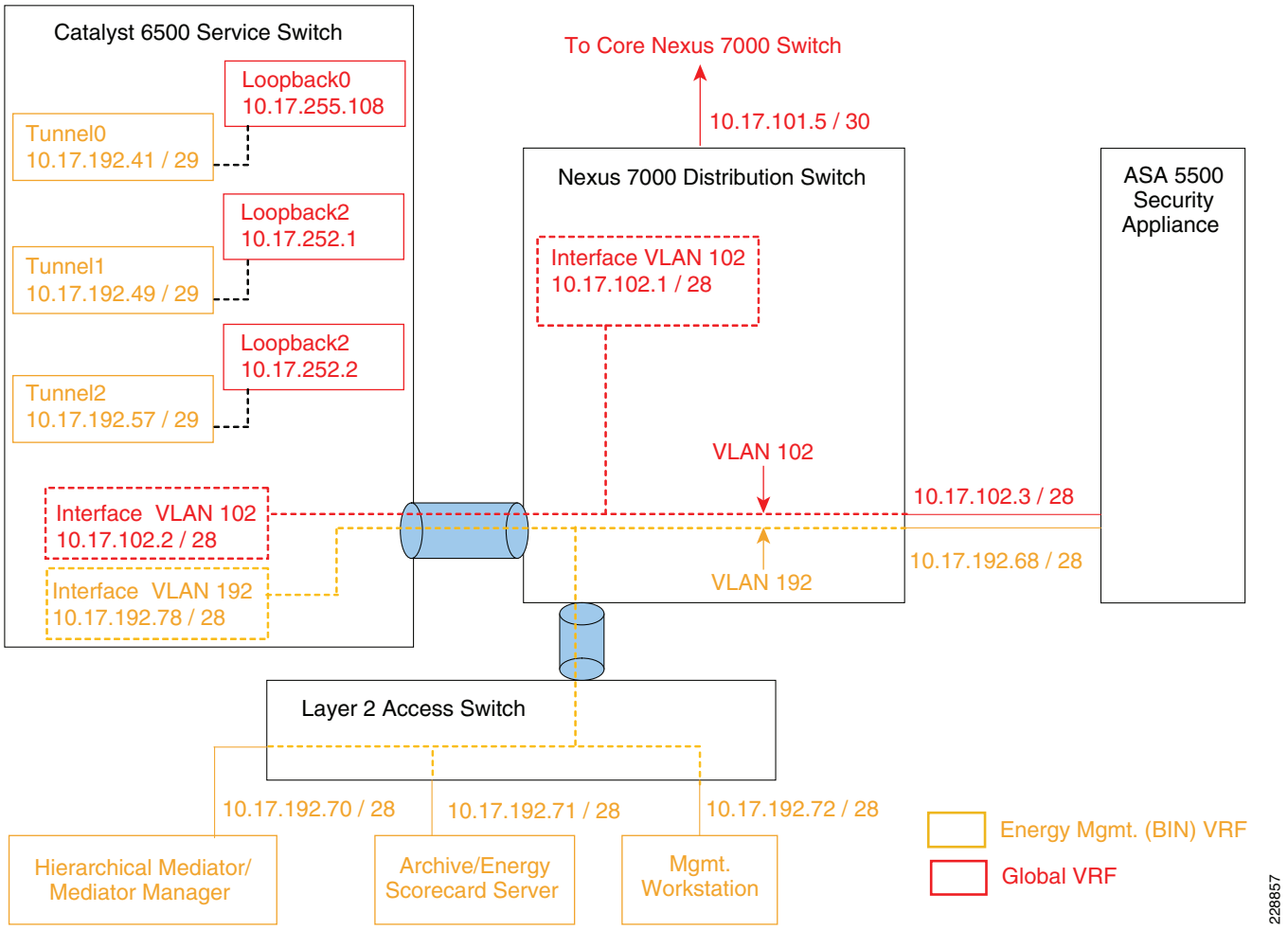
The following describes the numbers in Figure 5-13:

- **1**—EMOC VLAN trunked through Nexus 7000 Distribution Switch to the Catalyst 6500 Service Switch.
- **2**—GRE tunnels from Partner Extranet Module, Campus Building Modules, and WAN Edge Module terminate on Catalyst 6500 Service Switches; extending the BIN VRF across the campus network to these locations.
- **3**—Hierarchical Mediator functionality can provide a real-time single point of access to energy usage information (datapoints) from Mediators deployed throughout the enterprise network.
- **4**—Internal enterprise archive servers may collect periodically exported datapoint information from individual Mediators deployed throughout the network infrastructure. An energy scorecard service may make historical energy usage information available internally within the organization.

- **5**—Internal enterprise management workstations may be used to configure the hierarchical and/or remote Mediators; deploy logical control applications to the hierarchical and/or remote Mediators; and to create, monitor, and deploy websites to the hierarchical and/or remote Mediators.

In this example, a separate EMOC VLAN is again implemented within the Data Center Service Module. The EMOC VLAN is trunked from the access switch, through the Nexus 7000 Series Distribution Switch, to a Layer-3 interface defined within the Catalyst 6500 Service Switch. The Layer-3 interface sits on the BIN VRF, separate from the global VRF which houses the rest of the enterprise data network. GRE tunnels are then defined on the Catalyst 6500 Service Switch, which extend the BIN VRF out into the campus network. Figure 5-14 shows a more detailed view, without redundancy for clarity of the drawing.

Figure 5-14 Detailed Example Data Center Service Module Design Using VRF-Lite with GRE Tunnels



Example 5-1 provides a partial configuration from the Catalyst 6500 Service Switch.

Example 5-1 Partial Configuration Catalyst 6500 Service Switch with VRFs and GRE Tunnels

```
!
ip vrf bin
! Creates Building Infrastructure Network (BIN) VRF
rd 192:108
!
~
!
interface Tunnel0
! GRE Tunnel to Partner Extranet Module
description VRF FOR MEDIATOR NETWORK TO ME-EASTDIST-1
ip vrf forwarding bin
ip address 10.17.192.41 255.255.255.248
tunnel source Loopback4
tunnel destination 10.16.255.40
!
interface Tunnel1
! GRE Tunnel to Campus Building Module
description VRF FOR MEDIATOR NETWORK TO ME-WESTCAMP-1
ip vrf forwarding bin
ip address 10.17.192.49 255.255.255.248
tunnel source Loopback2
tunnel destination 10.17.255.51
!
interface Tunnel2
! GRE Tunnel to WAN Edge Module
description VRF FOR MEDIATOR NETWORK TO ME-WESTDIST-1
ip vrf forwarding bin
ip address 10.17.192.57 255.255.255.248
tunnel source Loopback0
tunnel destination 10.17.252.3
!
interface Loopback0
description LOOPBACK INTERFACE FOR TUNNEL FROM ME-WESTDIST-1
ip address 10.17.255.108 255.255.255.255
!
interface Loopback2
description LOOPBACK INTERFACE FOR TUNNEL FROM ME-WESTCAMP-1
ip address 10.17.252.1 255.255.255.255
!
interface Loopback4
description LOOPBACK INTERFACE FOR TUNNEL FROM ME-EASTDIST-1
ip address 10.17.252.2 255.255.255.255
!
~
!
interface TenGigabitEthernet1/2
! Trunk to Nexus 7000 Data Center Distribution Switch
description TRUNK TO ME-WESTDC7K-1
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
load-interval 30
wrr-queue bandwidth 5 25 10 10 5 5 10
priority-queue queue-limit 30
wrr-queue queue-limit 5 25 10 10 5 5 10
wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 3 80 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 4 80 100 100 100 100 100 100 100
```

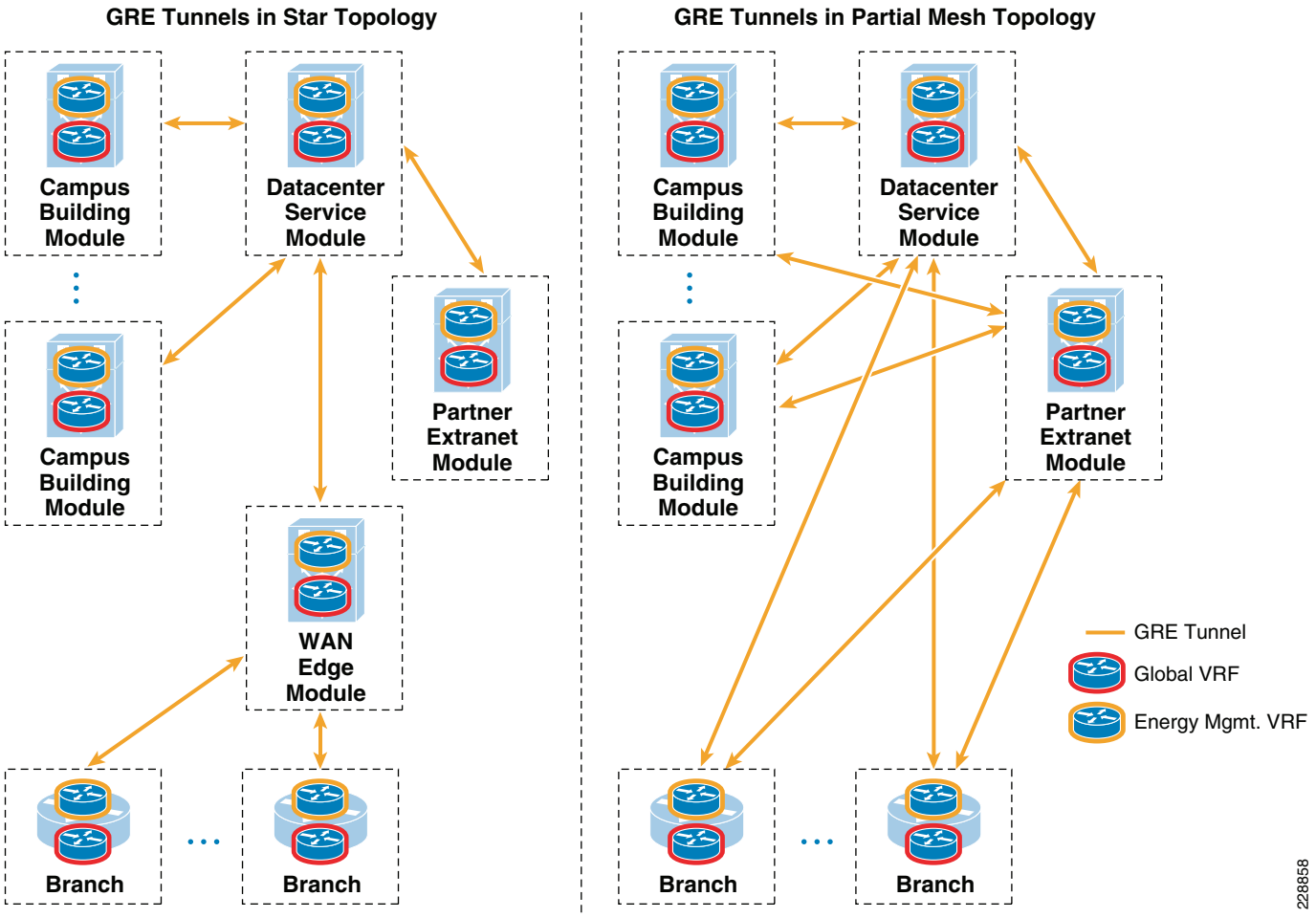
```
wrr-queue random-detect min-threshold 5 80 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 6 80 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue cos-map 1 1 1
wrr-queue cos-map 2 1 0
wrr-queue cos-map 3 1 2
wrr-queue cos-map 4 1 3
wrr-queue cos-map 5 1 6
wrr-queue cos-map 6 1 7
wrr-queue cos-map 7 1 4
mls qos trust dscp
!
~
!
interface Vlan102
! Extends DataCenter Global VRF to Cat6K Service Switch
ip address 10.17.102.2 255.255.255.240
!
interface Vlan192
! Extends DataCenter BIN VRF to Cat6K Service Switch
ip vrf forwarding bin
ip address 10.17.192.78 255.255.255.240
standby 1 ip 10.17.192.76
standby 1 priority 90
!
~
!
router eigrp 111
network 10.17.0.0 0.0.255.255
no auto-summary
!
address-family ipv4 vrf bin
! Creates EIGRP instance for BIN VRF
autonomous-system 99
network 10.17.192.0 0.0.0.255
network 10.17.252.0 0.0.0.255
network 10.17.255.0 0.0.0.255
exit-address-family
!
```

In the above example, separate GRE tunnels are provisioned, extending the BIN VRF to the Catalyst 6500 Series Distribution Switches within the following campus locations:

- *Partner Extranet Module*—This places inbound remote-access or site-to-site VPN traffic from the MSP partner onto the BIN VRF, effectively isolating it from the rest of the enterprise traffic.
- *WAN Edge Module*—This extends the BIN VRF to the WAN edge. A separate set of GRE tunnels then extends the BIN VRF out to each remote branch which houses a Mediator.
- *Campus Building Modules*—This extends the BIN VRF to each campus building which houses a Mediator.

The deployment of GRE tunnels which start out from the Data Center Service Module may provide a somewhat more manageable deployment for enterprise and partner access to the Mediators than provisioning tunnels directly from the Partner Extranet Module to each Mediator location within the campus or branches. An example of this is shown in Figure 5-15.

Figure 5-15 Star vs Partial-Mesh Deployment of GRE Tunnels



As shown in Figure 5-15, the overall number of GRE tunnels that must be provisioned is less with the star configuration versus the partial-mesh configuration. Note that Figure 5-15 does not show redundant GRE tunnels, which connect between the redundant Catalyst 6500 switch pairs. Catalyst 6500 switches handle GRE tunneling in hardware and, therefore, provide a platform sufficient for moderate-sized VRF deployments in this configuration. Further, with a star configuration, all traffic is routed back toward the Data Center Service Module before being routed out toward the remote branch and campus Mediators. This design facilitates the use of a hierarchical Mediator/Mediator Manager deployed within the data center EMOC. Since the BIN VRF is assumed to be dedicated to the energy management solution, no additional firewalling is shown within the datacenter between the EMOC and the rest of the energy management solution. Stateful access control at both the VPN concentrator and firewall within the Partner Extranet Module already restricts access from MSP partner devices. If desired, ACLs could be deployed across the GRE tunnel interfaces of the Catalyst 6500 Service Switches to further restrict access within the BIN VRF. This may be useful if the network virtualization concept is expanded to include other functionality such as video surveillance and physical access control, as well as energy management, into a single BIN VRF.

Other methods exist for providing VRF connectivity to the Data Center Service Module. These include the use of multipoint GRE tunnels that may be used to dynamically establish connectivity directly between tunnel endpoints. This may provide a more scalable deployment. Alternatively, an end-to-end

VRF-Lite implementation may be deployed in which the BIN VRF is extended throughout the Nexus 7000 data center switches as well as the campus core and Distribution Switches. Future revisions of this design guide may include designs using these technologies.

Client PC Access when Deploying a VRF for the Energy Management Solution

When deploying a VRF for the energy management solution, access control between enterprise client PCs located on the global VRF and devices on the energy management VRF should ideally be restricted to one point, or, alternatively, a small handful of points within the network infrastructure. Otherwise, the whole concept of implementing a VRF for path isolation becomes somewhat irrelevant. This also eases the administrative burden of not having to configure and manage multiple stateful firewalls deployed throughout the enterprise network when network virtualization is not implemented.

Chapter 4, "Internet Edge Design Considerations" discusses how MSP partner workstations that access the network via remote-access VPN or site-to-site VPN can gain access to the energy management VRF. This represents one access point into the energy management VRF. Therefore, one possible method of allowing enterprise client PCs access to the Mediators, when deploying a VRF, is also through the Partner Extranet Module. This could be accomplished by having the enterprise client PCs establish remote-access IPSec VPN connections to the BIN VRF via the same remote-access VPN device (in this case the ASA 5500 Series Security Appliances within the Partner Extranet Module) as MSP partner workstations. The advantage of this design is that all access into the BIN VRF, regardless of whether it is a partner workstation or enterprise client PC, is established through a single set of devices. In this case, the devices are the ASA 5500 Security Appliances deployed within the Partner Extranet Module. AAA services on the ASA 5500 Security Appliance can be used to centralize access control via RADIUS to a AAA server such as the Cisco Secure ACS server, which in turn may rely on a backend directory server or LDAP database. The disadvantage of this design is that it forces enterprise client PC traffic into the Partner Extranet Module; therefore, it violates the design paradigm of separation of partner and employee traffic at the Internet edge. Further, routing IPSec VPN traffic from enterprise client PCs into the Partner Extranet Module, where it is then decrypted and routed back into the BIN VRF, may be somewhat challenging.

Alternatively, a stateful firewall deployed within the Data Center Service Module (either a FWSM or ASA 5500 Security Appliance) can serve as a point of access control between the global VRF and the BIN VRF, as is shown in Figure 5-14 on page 5-15. The network administrator should still consider the use of remote-access IPSec VPN connections from the enterprise client PCs to the BIN VRF. This is one advantage of implementing an ASA 5500 Security Appliance over the Catalyst 6500 FWSM. This design has the advantage of maintaining the design paradigm of separating partner traffic from employee traffic at the Internet edge. Also, this design may be somewhat simpler to implement if the firewall already exists for E-mail (SMTP) traffic generated by the Mediators to be sent to corporate E-mail servers; or if the Mediators need to use corporate DNS servers. However, the disadvantage of this design is that there are effectively two access control points into the BIN VRF; one at the Internet edge for partner traffic and one within the data center for internal traffic. Note that the deployment of the hierarchical Mediator or internal energy management scorecard server on a DMZ segment can also be deployed with a VRF design, using the data center firewall.

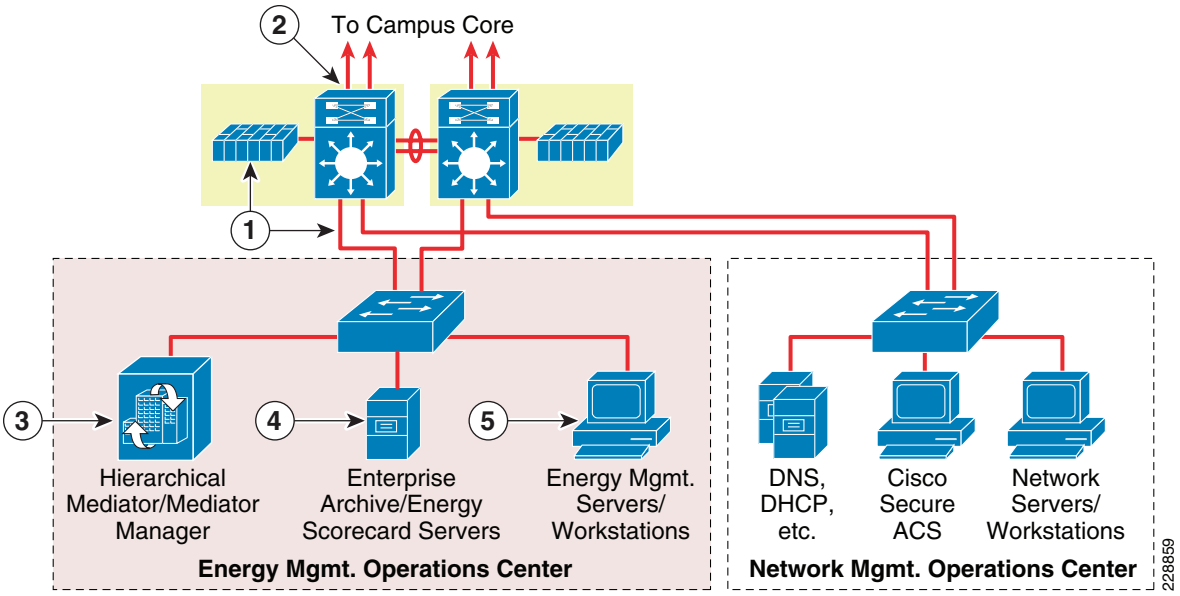
Campus Service Module Design

In other situations, the facilities management personnel are not physically located within the data center of the campus or the campus location does not have a data center housed within it. In these scenarios, a separate Campus Service Module hanging off the Campus Core Module can be implemented for the EMOC. Again, both non-VRF and VRF designs can be implemented.

Non-VRF Campus Service Module Designs

The designs for the Campus Service Module are similar to the Data Center Service Module designs, but with some differences in the switching infrastructure. Figure 5-16 shows an example of a non-VRF Campus Service Module design with Catalyst 6500 Service Switch and FWSM

Figure 5-16 Campus Service Module Design with Catalyst 6500 Switch and FWSM



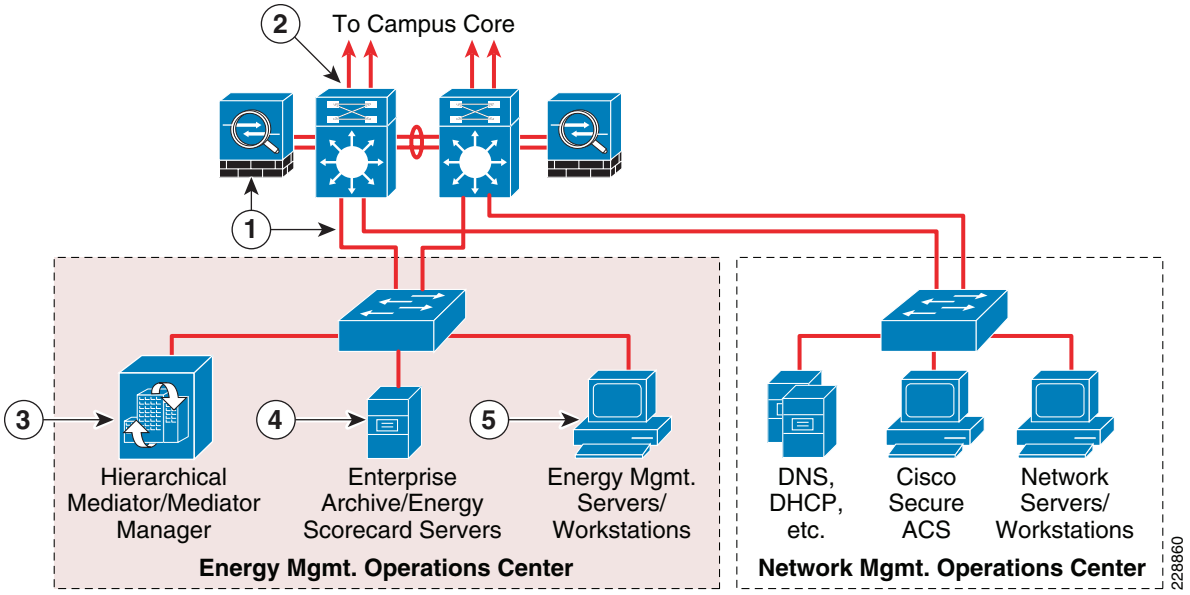
The following describes the numbers in Figure 5-16:

- **1**—EMOC VLAN trunked through Catalyst 6500 Distribution Switch to the FWSM.
- **2**—FWSM in the Catalyst 6500 Distribution Switch provides stateful access control to and from the EMOC devices.
- **3**—Hierarchical Mediator functionality can provide a real-time single point of access to energy usage information (datapoints) from Mediators deployed throughout the enterprise network.
- **4**—Internal enterprise archive servers may collect periodically exported datapoint information from individual Mediators deployed throughout the network infrastructure. An energy scorecard service may make historical energy usage information available internally within the organization.
- **5**—Internal enterprise management workstations may be used to configure the hierarchical and/or remote Mediators; deploy logical control applications to the hierarchical and/or remote Mediators; and to create, monitor, and deploy websites to the hierarchical and/or remote Mediators.

In this example, the EMOC VLAN is trunked from the access switch to a Layer-3 interface on the FWSM module. However, the FWSM is located within the Catalyst 6500 Distribution Switch within the Campus Service Module, as opposed to a separate Catalyst 6500 Service Switch. The FWSM provides stateful access control to and from the EMOC VLAN. Again, note that there are many different ways in which firewalling of the EMOC VLAN could be achieved within the Campus Service Module, because the FWSM supports both transparent (Layer 2) and routed mode (Layer 3) firewalling, high-availability through active/active or active/standby firewall configurations, and single or multiple context (virtual firewalls) mode. This example shows only one highly simplified method using a single context, routed mode firewall in an active/standby configuration.

As with the data center design, an alternative to the FWSM design is to implement a set of ASA 5500 Security Appliances within the Campus Service Module, as shown in Figure 5-17.

Figure 5-17 Non-VRF Campus Service Module Design with Catalyst Distribution Switch and ASA 5500 Security Appliance



The following describes the numbers in Figure 5-17:

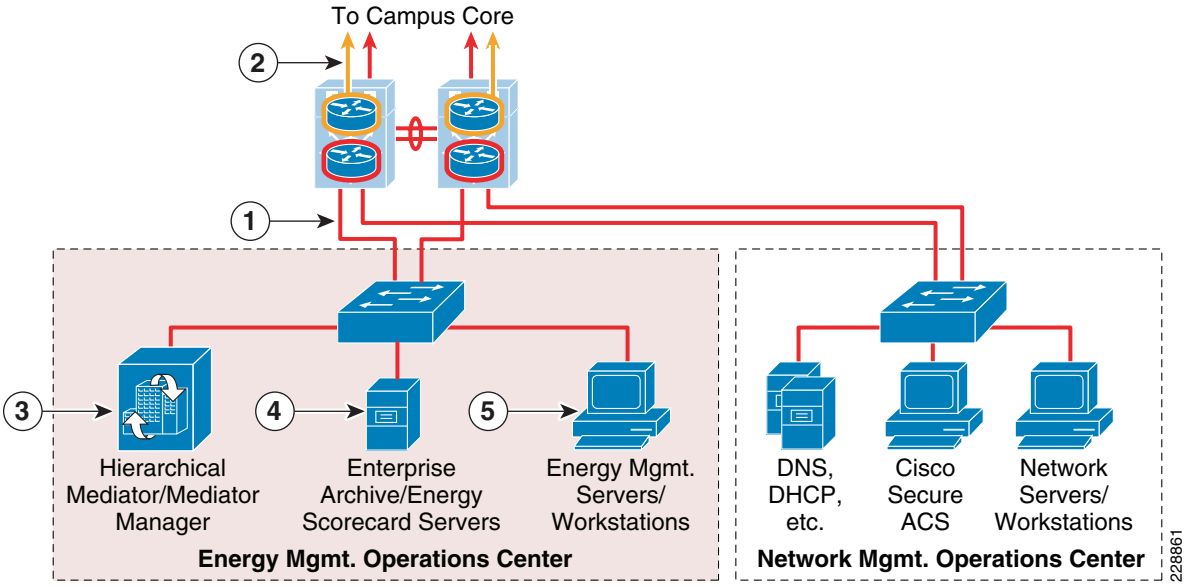
- **1**—EMOC VLAN trunked through Catalyst Distribution Switch to the ASA 5500 Security Appliance.
- **2**—ASA 5500 Security Appliance provides stateful access control to and from the EMOC devices.
- **3**—Hierarchical Mediator functionality can provide a real-time single point of access to energy usage information (datapoints) from Mediators deployed throughout the enterprise network.
- **4**—Internal enterprise archive servers may collect periodically exported datapoint information from individual Mediators deployed throughout the network infrastructure. An energy scorecard service may make historical energy usage information available internally within the organization.
- **5**—Internal enterprise management workstations may be used to configure the hierarchical and/or remote Mediators; deploy logical control applications to the hierarchical and/or remote Mediators; and to create, monitor, and deploy websites to the hierarchical and/or remote Mediators.

In this design, the EMOC VLAN is trunked from the access switch, through the Campus Service Module Distribution Switch, to a Layer-3 interface off of the ASA 5500 Security Appliance. One advantage of this design is that a wider range of switches (Catalyst 6500 Series, Catalyst 4500 Series, or even the Catalyst 3750 Series switch stack) can be used as the Campus Service Module switch. The ASA 5500 provides stateful access control to and from the EMOC VLAN. Again, note that there are many different ways in which firewalling of the EMOC VLAN could be achieved within the Campus Service Module, because the ASA 5500 Series supports both transparent (Layer 2) and routed mode (Layer 3) firewalling, high-availability through active/active or active/standby firewall configurations, and single or multiple context (virtual firewalls) mode. This example shows only one highly simplified method using a single context, routed mode firewall in an active/standby configuration. Individual interfaces or VLAN sub-interfaces could be used on the ASA 5500. Finally, as with the data center designs, other VLANs such as a Network Operations Center (NOC) VLAN can also be supported off of the same Campus Service Module.

VRF Campus Service Module Designs

Figure 5-18 shows an example of a Campus Service Module which makes use of VRFs to isolate the EMOC to a separate energy management VRF called the Building Infrastructure Network (BIN) VRF.

Figure 5-18 VRF Campus Service Module Design

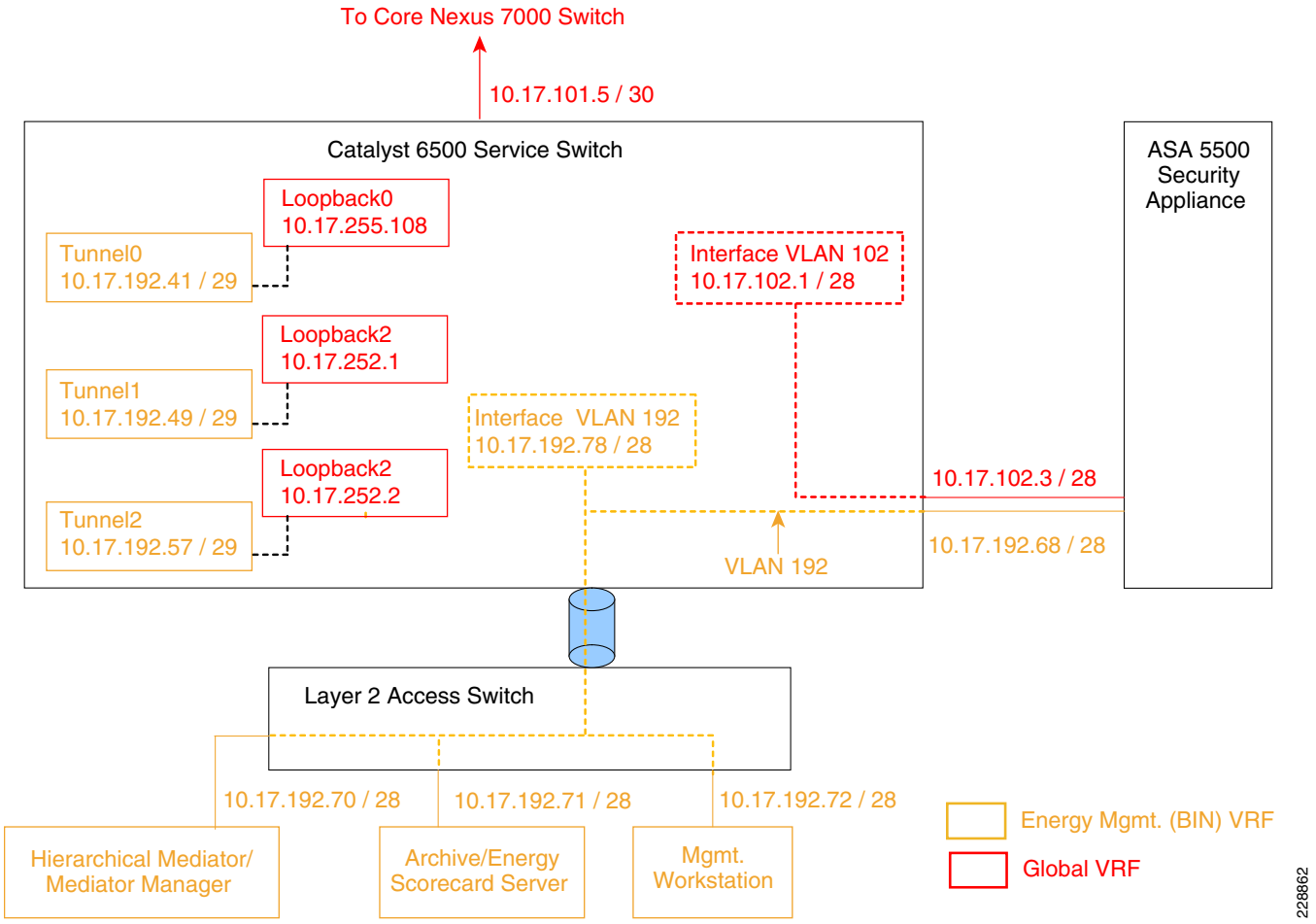


The following describes the numbers in Figure 5-18:

- **1**—EMOC VLAN trunked to the Catalyst 6500 Service Switch.
- **2**—GRE tunnels from Partner Extranet Module, Campus Building Modules, and WAN Edge Module terminate on Catalyst 6500 Campus Service Switches; extending the BIN VRF across the campus network to these locations.
- **3**—Hierarchical Mediator functionality can provide a real-time single point of access to energy usage information (datapoints) from Mediators deployed throughout the enterprise network.
- **4**—Internal enterprise archive servers may collect periodically exported datapoint information from individual Mediators deployed throughout the network infrastructure. An energy scorecard service may make historical energy usage information available internally within the organization.
- **5**—Internal enterprise management workstations may be used to configure the hierarchical and/or remote Mediators; deploy logical control applications to the hierarchical and/or remote Mediators; and to create, monitor, and deploy websites to the hierarchical and/or remote Mediators.

In this example, a separate EMOC VLAN is implemented within the Campus Service Module. The EMOC VLAN is trunked from the access switch to a Layer-3 interface defined within the Catalyst 6500 Service Switch. The Layer-3 interface sits on the BIN VRF, separate from the global VRF which houses the rest of the enterprise data network. GRE tunnels are then defined on the Catalyst 6500 Service Switch, which extend the BIN VRF out into the campus network. Figure 5-19 shows a more detailed view, without redundancy for clarity of the drawing.

Figure 5-19 Detailed Example Campus Service Module Design Using VRF-Lite with GRE Tunnels



As with the Data Center Service Module VRF design, access control between the BIN VRF and global VRF can be accomplished via a ASA 5500 Security Appliance deployed within the Campus Service Module. Again, the use of remote-access IPSec VPN on the ASA 5500 can be implemented as an added security measure for enterprise client PCs who require direct access to either the hierarchical Mediator, or remote Mediators deployed throughout the network infrastructure.