CHAPTER 4

Internet Edge Design Considerations

The Internet edge design provides three main services for the Cisco Network Building Mediator deployment:

- Internet connectivity through which logged data is exported from the Mediators to cloud services partners who provide features such as energy scorecards. Internet connectivity may also be used for interactive data exchanges to support capabilities such as automated demand response (ADR).
- VPN connectivity through which managed service provider (MSP) partners connect to the enterprise network in order to manage Mediator deployments.
- The Internet edge maintains strict access control to the Mediator deployment from devices outside the enterprise network

Internet edge designs vary considerably between organizations, and are often driven by the existing security policy of the particular business entity. Large enterprise organizations often separate employee Internet connectivity from partner connectivity through the deployment of separate network modules. Within each module, functionality may be converged onto a single device or separated onto multiple devices. This type of separation of access between employees and partners, and separation of functionality onto multiple devices, can provide more granular control of partner access to the enterprise, and is consistent with current Cisco SAFE best practices. For further information regarding network security best practices, the reader is encouraged to review the *Cisco SAFE Reference Guide* which can be found at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html

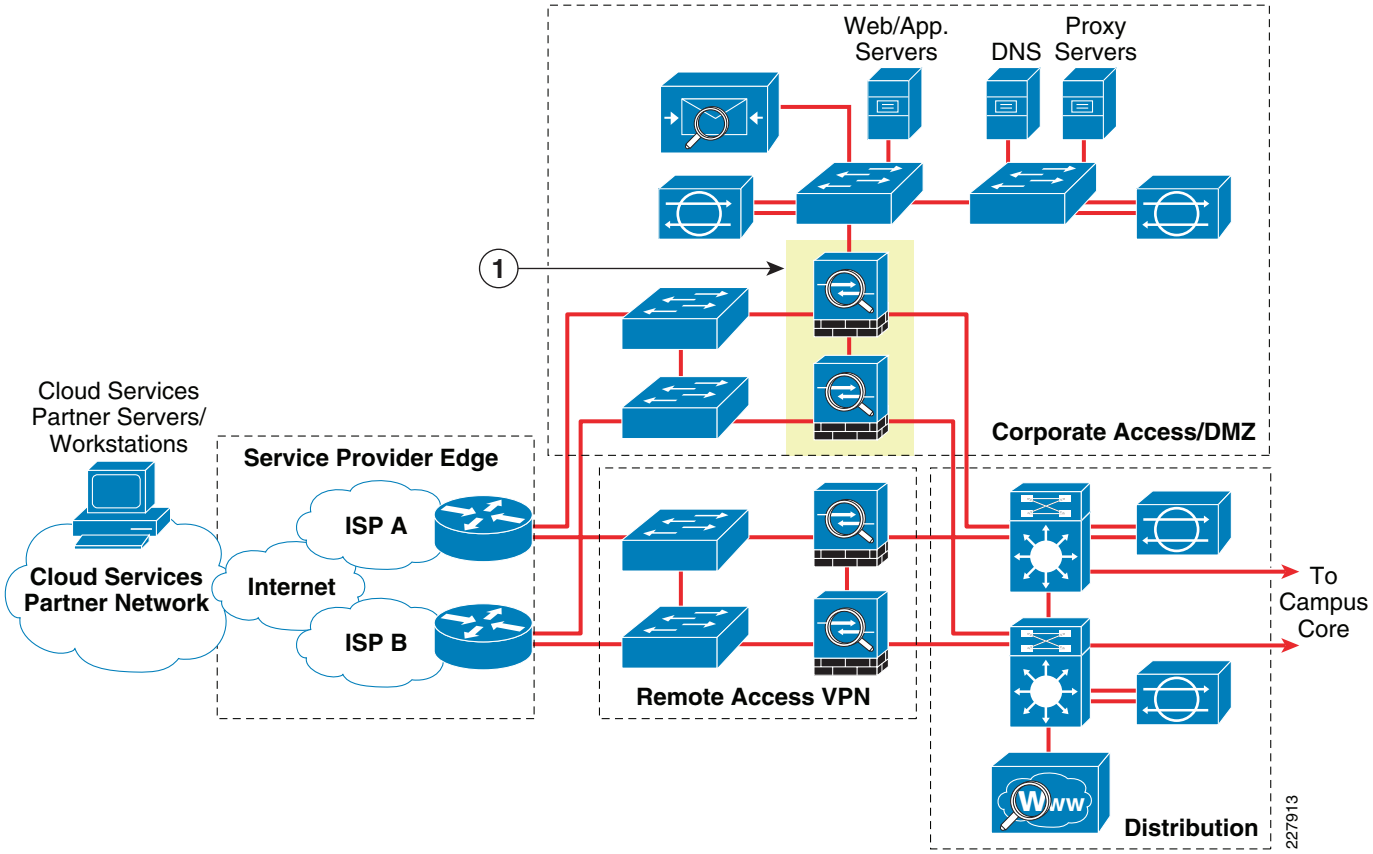
The Internet edge designs presented in this guide follows this design paradigm; presenting an overall Internet edge design for large organizations, with a separate Internet Edge Module and Partner Extranet Module, and separate devices for each functionality. However, for smaller organizations, a collapsed Internet edge design, where a single Internet Edge Module is deployed for both employee and partner access, is also discussed. In this design, all functionality is collapsed into a single device. These two design options represent both extremes (complete separation of functionality versus complete convergence of functionality) of Internet Edge designs. Actual Internet Edge designs typically lie somewhere between the two designs presented within this document.

Internet Edge Module

With respect of the energy management solution, the function of the Internet Edge Module is to provide stateful access control for outgoing connections initiated by the Mediators to cloud services partner servers accessible via the Internet. This is typically for the periodic exporting of logged data from the Mediators. However, the network administrator should note that in certain scenarios (such as if network virtualization is implemented for the Mediator deployment), exporting of logged data may be supported

through the Partner Extranet Module. This is discussed further in the "Extending VRFs to the Partner Extranet Module" section on page 4-25. The Internet Edge Module also provides stateful access control for enterprise client PCs accessing web-based energy scorecards provided by cloud services partners reachable through the Internet. An example of a redundant Internet Edge Module design is shown in Figure 4-1. Only the highlighted components, which are relevant to the energy management solution, are discussed in this document.

Figure 4-1 Example Internet Edge Module



The following describes the number in Figure 4-1:

- 1—ASA 5500 Security Appliances deployed within the Corporate Access/DMZ section provides address translation and stateful access control for outgoing connections to cloud-services partners.

The internal IP addressing of the Mediators and client PCs within an enterprise network is typically hidden by translating it to Internet routable addressing via Network Address Translation (NAT) functionality within the Internet Edge Module. A redundant pair of ASA 5500 Series Security Appliances within the Corporate Access/DMZ section of the Internet Edge Module, highlighted in Figure 4-1, can provide the required address translation and stateful access control services within this module.

Note The network administrator should note that the remote access VPN section of the Internet Edge Module is intended for employee VPN access only. With this type of design, partner VPN access is instead handled within the Partner Extranet Module, discussed in the next section. This provides a clean separation of traffic between internal employees and partners accessing the enterprise network.

Examples of the connections that should be allowed through the ASA 5500 Security Appliances for energy management flows through the Internet Edge Module are shown in Figure 4-2, Figure 4-6, and Figure 4-7.

Figure 4-2 Data Export From Mediators Directly to Cloud Services Partner Servers

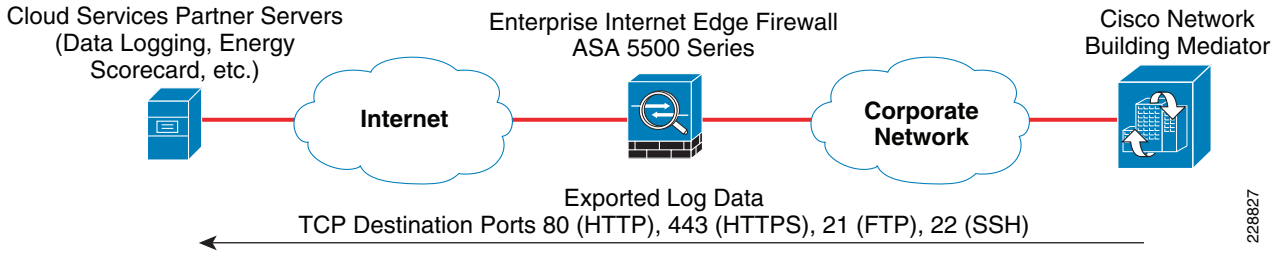


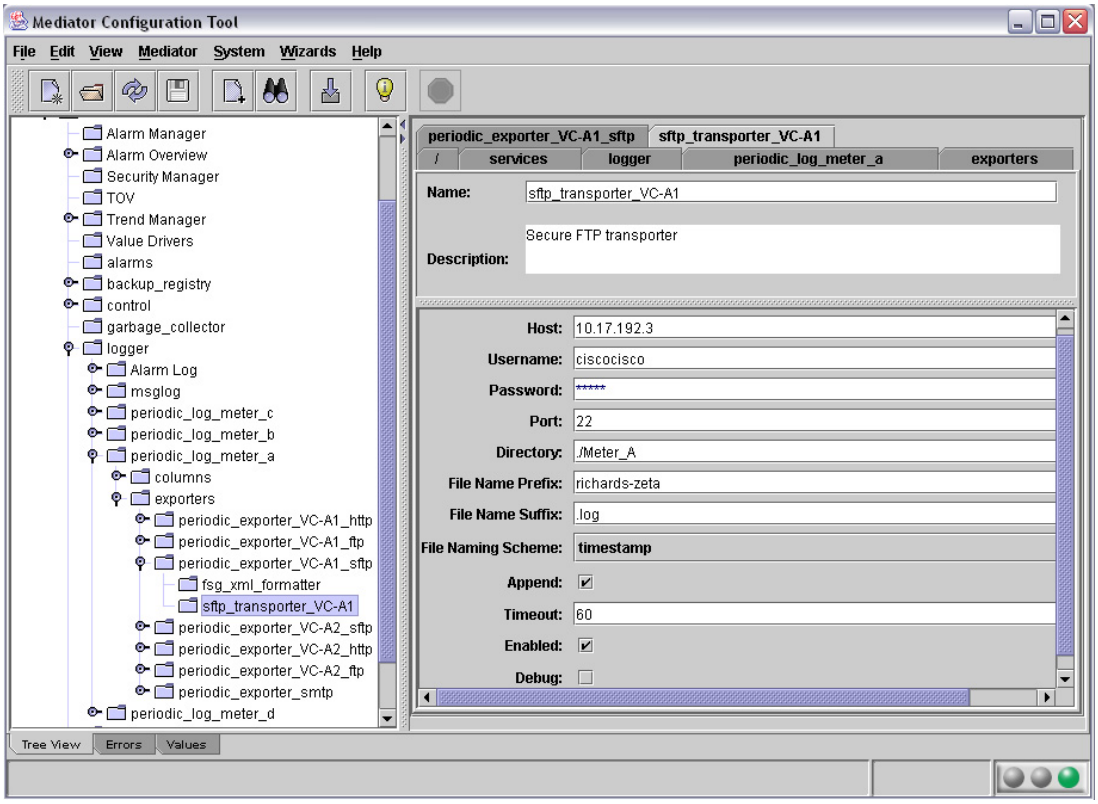
Figure 4-2 shows that the export of periodic-logged data is initiated by Mediators outbound toward the cloud-services partner servers. The Mediator is capable of exporting periodic-logged data via HTTP or HTTPS POST, FTP, or Secure FTP (SFTP) which uses the SSH protocol. Multiple data loggers and exporters can be configured within a single Mediator. However, in typical deployments, only one protocol is used for the data exports. Which protocol or protocols are used often depends on what the cloud-services partner can support, as well as what is acceptable to the enterprise organization.

Note The Mediator is also capable of exporting data via HTTP or HTTPS GET. However, this requires the cloud-services partner server to initiate an inbound connection through the Internet edge firewall directly to the Mediator. Due to the security implications of allowing an inbound connection into the enterprise network directly to the Mediator, this is not a highly recommended method of data export. The reader should also note that the Mediator shown in figures throughout this chapter can refer to remote Mediators deployed throughout branch and campus buildings; a hierarchical Mediator (as discussed within the Chapter 5, "Data Center/Campus Service Module Design Considerations") deployed within the Energy Management Operations Center (EMOC); or the future Cisco Network Building Mediator Manager appliance.

When using FTP for data export, the ASA 5500 Series Security Appliance will inspect the FTP control channel to dynamically open the data channel necessary for the actual file transfer. This is one of the benefits of implementing a stateful firewall with application-layer inspection capabilities at the Internet Edge. Application-layer inspection reduces the security holes created by having to statically open high-order port ranges in order to accommodate the randomly chosen data channel. Noted that FTP sends traffic unencrypted, including userids and passwords. For greater security, the network administrator should consider working with its cloud-services partner to implement a secure alternative to FTP such as Secure FTP (SFTP). SFTP uses the Secure Sell (SSH) protocol in order to provide data authentication and encryption of the data export. Additionally, with SFTP, the network administrator no longer has to be concerned with separate control and data channels. Likewise, when using HTTP POST for data export, the network administration should consider working with its cloud-services partner to implement HTTPS POST as an alternative, because HTTPS uses SSL/TLS to provide data authentication and encryption.

For each of the data exporters (HTTP or HTTPS POST, FTP, or SFTP), a username and password can and should be configured within the Mediator. An example of this is shown in Figure 4-3, which shows an SFTP transporter.

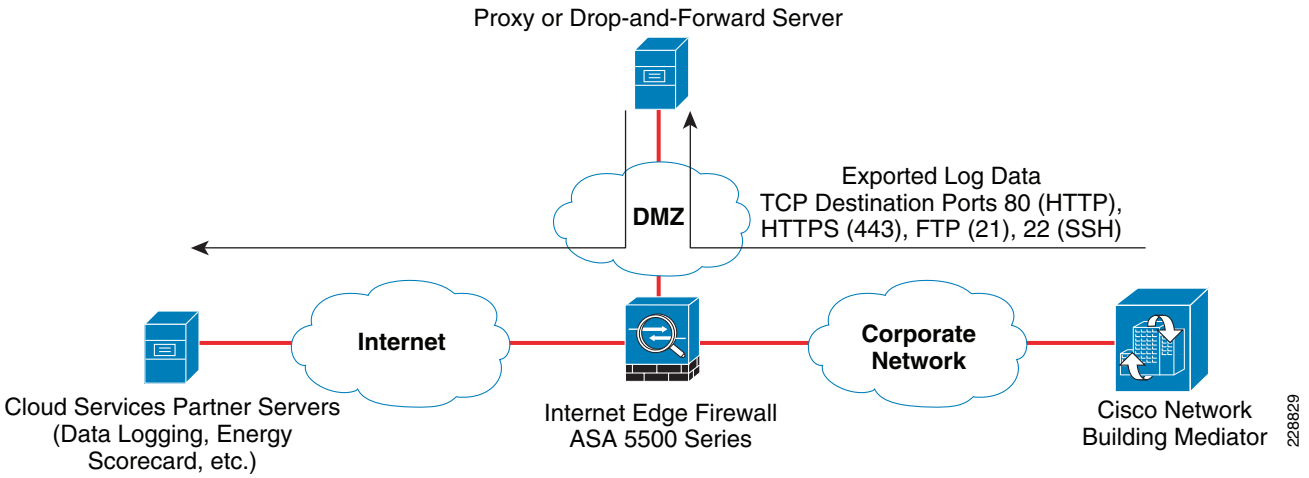
Figure 4-3 Example Configuration of a Username and Password for Data Export From Mediators to Cloud Services Partner Servers



The username and password are used to authenticate the Mediator to the particular server (HTTP, FTP, or SSH server) before transferring the log files that contain datapoint information. The use of a unique username and password for the data export from each Mediator may be considered, versus using the same username and password configured for all Mediators within a deployment. The benefit to this approach is that if the username and password of a single Mediator is compromised, then only that particular username and password needs to be changed on both the Mediator and the cloud services partner server; versus having to change the usernames and passwords of all of the Mediators. The downside to this approach is that it can result in significantly more administrative overhead. Again, the network administrator should consider working with its cloud-services partner in order to determine if the additional security benefits outweigh the administrative overhead of maintaining separate usernames and passwords for data export from each Mediator.

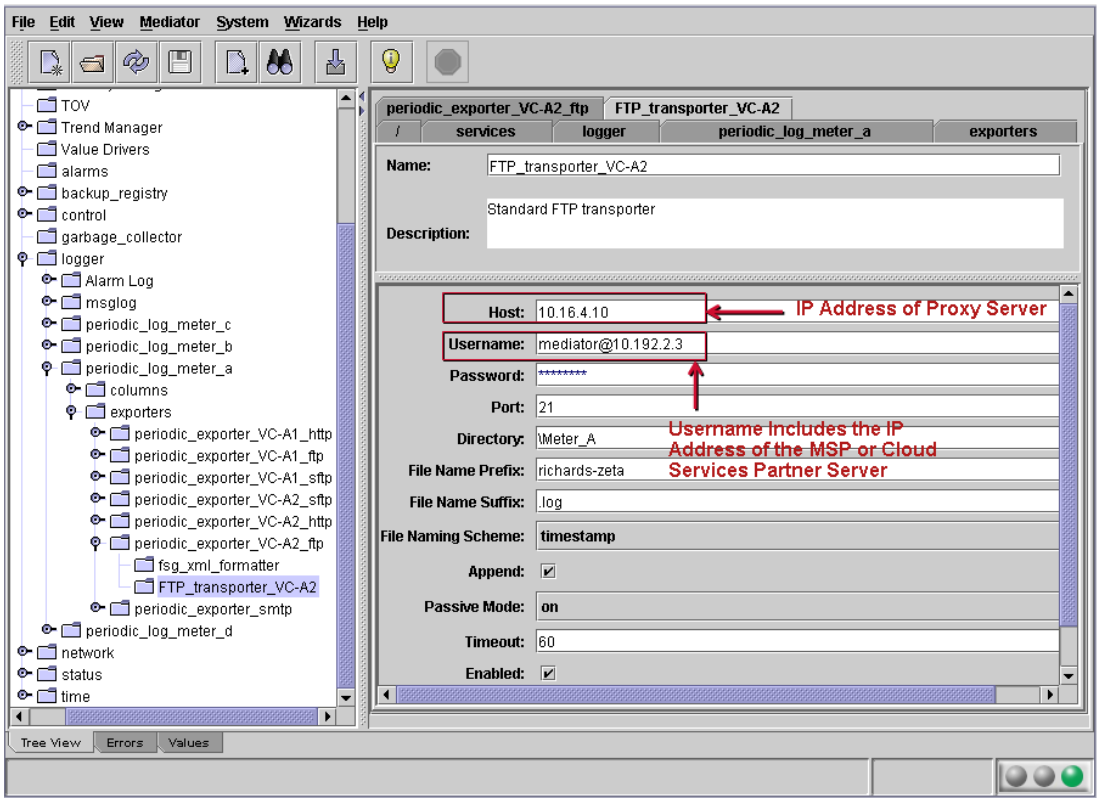
Another alternative is to export log files from multiple Mediators through a secure proxy server located within the Corporate Access/DMZ section of the Internet Edge Module. An example of this is shown in Figure 4-4.

Figure 4-4 Data Export From Mediators to Cloud Services Partner Servers via Proxy or Drop-and-Forward Server



When configuring an FTP exporter within the Mediator to use a proxy server, the configuration may need to be modified, as shown in Figure 4-5.

Figure 4-5 Example Configuration for Data Export From Mediators to Cloud Services Partner Servers via FTP Proxy Server



As shown inFigure 4-5 above, the host field has been modified to point to the IP address of the FTP proxy server located within the DMZ of the enterprise network. Note that a hostname can be used, if DNS resolves the hostname to an IP address. The username field has also been modified to include the username as well as specifying the IP address of the actual cloud services partner server. This is

accomplished via the use of the @ symbol. This configuration can be used to allow the FTP proxy server to automatically "forward" the exported data logs from the Mediators to the cloud-services partner servers.

Note A basic FTP proxy design was tested for this design guide using the ftp.proxy FTP proxy-server (http://www.ftpproxy.org/) running on a Fedora Linux server.

Using an FTP proxy server has the advantage in that the FTP proxy server itself is the only device that establishes an FTP connection outside the corporate network to the cloud-services partner server for data export. Firewall configurations can therefore be tightened somewhat to allow only the FTP proxy server or servers out, versus allowing every Mediator to individually establish FTP sessions out. The network administrator should note, however, that similar benefits are derived from a firewall, such as the Cisco ASA 5500 Series Security Appliance, running application-layer inspection of FTP and using NAT to hide the internal IP addressing of the Mediators. In large Mediator deployments, the scalability of the FTP proxy server or servers should be thoroughly assessed, in order to ensure that they do not result in a bottleneck for data exports from the energy management solution. The FTP proxy server itself should also be thoroughly hardened, due to its placement on the DMZ segment of the firewall.

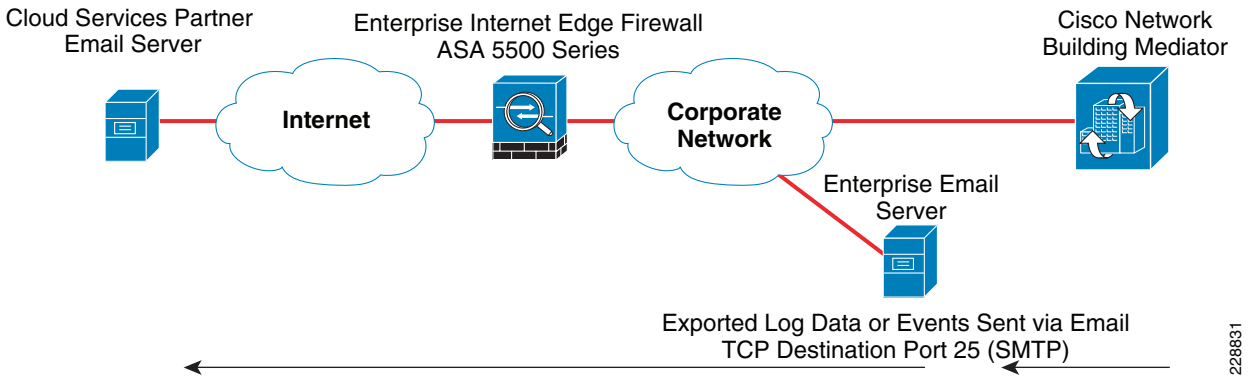
For protocols that may be difficult to proxy, such as SFTP that uses the SSH protocol, a drop-and-forward mechanism may be implemented. In this scenario, the Mediators export to a server sitting on a the firewall DMZ segment; which in turn, periodically exports to the cloud-services partner server. An alternative method is for the network administrator to work with their cloud services partner to determine if the cloud services partner can periodically establish a secure connection inbound to the drop-and-forward server and retrieve the log files exported by the Mediators. One advantage of this scenario is that a public/private key pair can be used to authenticate the enterprise drop-and-forward server to the cloud services partner server; instead of the username and password used by the Mediator currently. The username and password configured within the Mediator are still used, but only to authenticate to the drop-and-forward server sitting on a DMZ segment within the corporate network. Therefore, the decision whether to use a single password for exports from all Mediators within the deployment, or to use individual passwords for each Mediator; now shifts completely to the network administrator. The network administrator should note, however, that the additional drop-and-forward function can add additional delays in exporting log files to the cloud services partner. For business requirements that need frequent exporting of log data for near-real-time use, this may not be a feasible design. However, for business requirements that need very infrequent exporting of log data for long-term trending use, this may be a feasible design.

Note A basic drop-and-forward design was tested for this design guide using OpenSSH (http://www.openssh.com/) running on a Fedora Linux server, along with simple shell scripts and a cron job.

The network administrator should note that both the proxy or drop-and-forward functions add another layer of complexity, additional hardware, and additional software to the energy management solution design. The network administrator should carefully evaluate the additional advantages of deploying either of these methods against the potential additional costs of supporting such a design. Finally, note that the use of proxy or drop-and-forward servers for outbound sessions is often dictated by the security policy of the enterprise organization.

Figure 4-6 shows that the Mediator can also export either periodic logged data or event data, via E-mail, using the Simple Mail Transfer Protocol (SMTP).

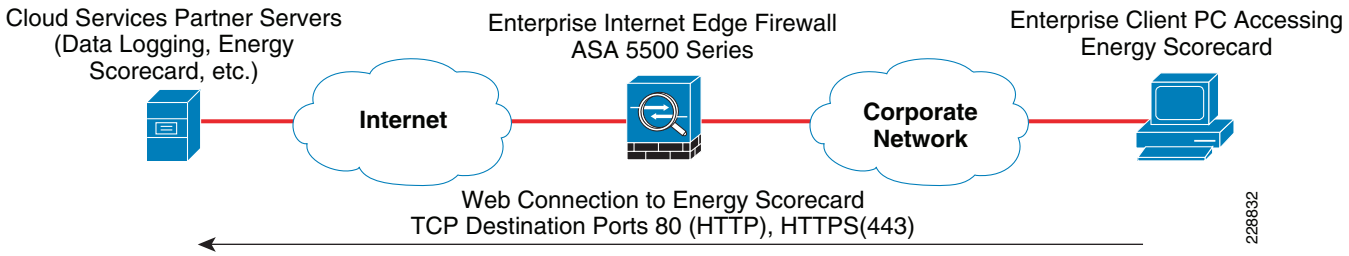
Figure 4-6 Data Export and/or Event Forwarding to Partners via E-mail



In this scenario the data originating from the Mediator is either embedded within the E-mail message or included as an attachment, and sent to the corporate E-mail servers. The logged data or event data can then be forwarded as normal E-mail from the enterprise E-mail servers to an account on the cloud services partner E-mail servers; passing through the ASA 5500 Security Appliances on the Internet edge. (Note that this example has been highly simplified from actual corporate E-mail systems.)

Figure 4-7 shows an example of an enterprise client PC accessing an energy scorecard located on a cloud services partner server, via a web browser.

Figure 4-7 Client PC Energy Scorecard Access



In this scenario, HTTP or HTTPS sessions initiated by client PCs need to be allowed outbound to the cloud services partner servers, through the ASA 5500 Series Security Appliance. As with the exporting of periodic logged data, the network administrator should consider working with the cloud services partner to implement HTTPS instead of HTTP in order to provide data authentication and encryption of the data flow. In addition, username and password protection of the energy scorecard site is highly recommended.

Note The port numbers for each of the service flows shown in Figure 4-2, Figure 4-6, Figure 4-7 are default values. These are configurable within the Cisco Network Building Mediator. The network administrator can choose to use different port numbers for HTTP, HTTPS, FTP, SFTP (SSH), and/or SMTP. if desired. Note that, however, changing the default ports may create issues with application-layer inspection within the Internet edge firewall, and is not highly recommended.

The actual configuration of the ASA 5500 firewall, in order to allow the exporting of periodic logged data or event data from the Mediators, as well as allow access from client PCs to the Energy Scorecard, is highly dependant upon the security policy of the organization. Security operations personnel should be involved within the discussions involving Cisco Network Building Mediator deployments. Some enterprise organizations allow all outbound connections directly to the Internet, but restrict inbound

connections. Other organizations limit direct outbound connections to certain protocols. Still other organizations may both limit outbound connections to certain protocols, and force client PCs through a proxy server for well known protocols such as HTTP and FTP. The following partial ASA 5500 firewall configuration (non-redundant) shows a very simplified example (see Example 4-1) where all direct outbound Internet access initiated by devices within the corporate network is allowed.

Example 4-1 Example of a Partial ASA 5500 Firewall Configuration for Internet Edge Access

```
!
interface GigabitEthernet0/1             ! Inside interface with higher security level.
 description CONNECTION TO ME-EASTDIST-1 G5/1
 nameif inside
 security-level 100
 ip address 10.16.2.2 255.255.255.252
!
interface GigabitEthernet0/3              ! Outside interface with lower security level.
 description CONNECTION TO OC3 INTERNET VIA ME-EASTINET-3 & 4
 nameif outside
 security-level 25
 ip address user_inet 255.255.255.248
!
~
!
access-list inside_nat_outbound extended permit ip any any
!                                          ! Causes all Inside addresses
!                                          ! to use NAT when connecting to Internet
hosts.
~
!
nat-control                                ! Enables NAT for Inside to Outside
connections.
!
!
global (outside) 1 interface               ! Uses the Outside Interface Address for the
global pool (PAT).
!
nat (inside) 1 access-list inside_nat_outbound   ! Specifies the NAT access-list for the
                                                 !Inside Interface.
!
~
!
class-map inspection_default               ! Specifies default class-map for
application-layer
 match default-inspection-traffic          ! inspection
!
policy-map global_policy                   ! Name of the inspection policy map
 class inspection_default
  inspect ftp                              ! Enables FTP inspection.
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect http
  inspect dns
```

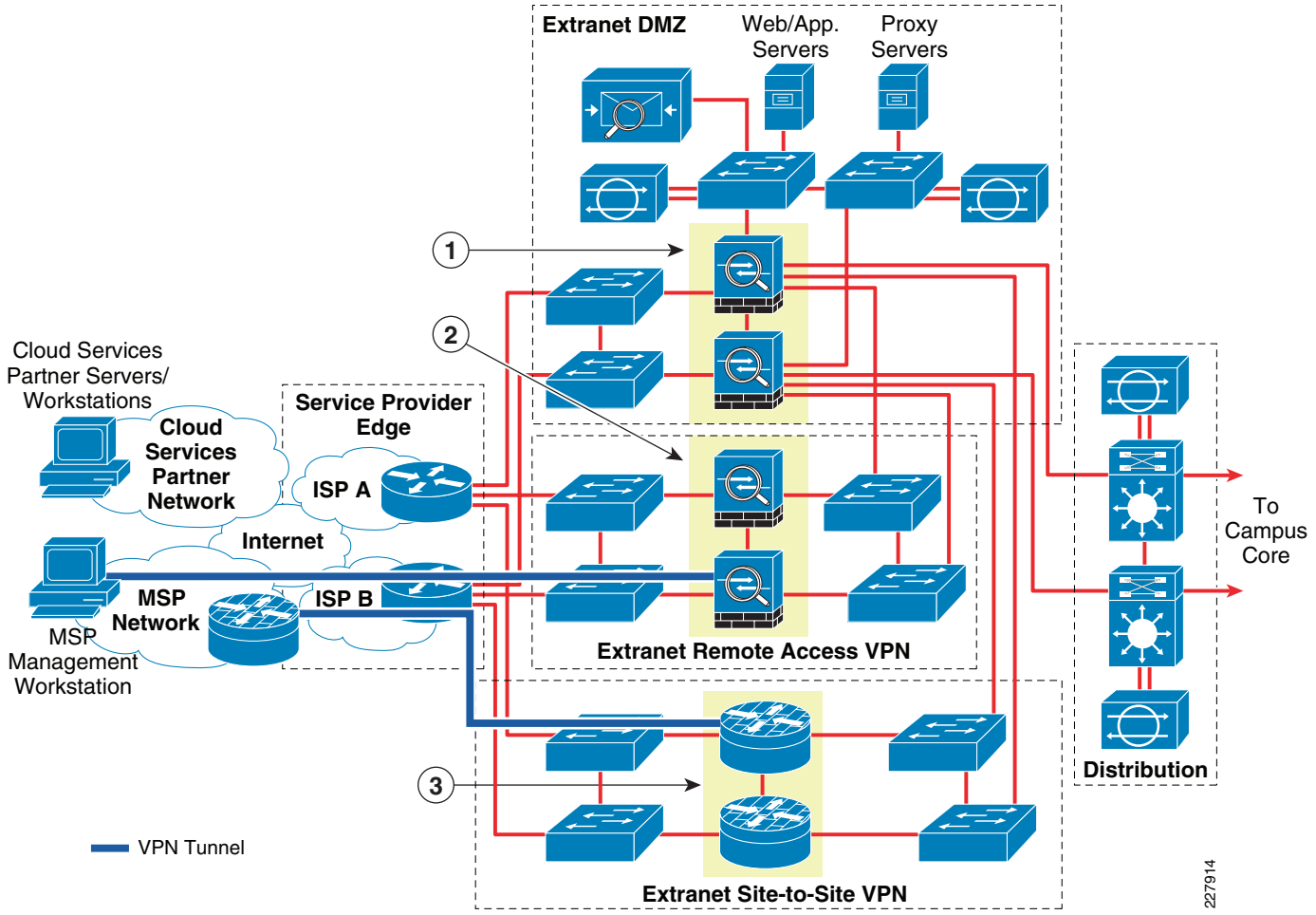
```
!
service-policy global_policy global         ! Applies global_policy map to the firewall.
!
```

By default, traffic from an interface with a lower security level to an interface with a higher security level is blocked by an implicit access-list, unless specifically allowed by a user-defined access-list applied inbound on the outside interface. Therefore, all inbound access initiated by devices on the Internet is blocked. By default, traffic from an interface with a higher security level to an interface with a lower security level is allowed by an implicit access-list, unless specifically denied by a user-defined access-list applied inbound on the Inside interface. Therefore, all outbound Internet access initiated by devices within the enterprise organization is allowed. In this example, all outbound connections use the IP address of the outside interface of the firewall, in a Port Address Translation (PAT) configuration. In larger organizations, typically a pool of IP addresses is defined, and a combination of NAT and/or PAT is used to provide network address translation from internal corporate addressing to external Internet routable addresses. This not only provides a more efficient means of using the existing Internet routable address space, but can also provide an additional layer of security by hiding the real internal addressing structure of the enterprise organization. Finally, application-layer inspection of protocols such as FTP is enabled, allowing the ASA 5500 firewall to inspect FTP control channels in order to dynamically open the required data channels.

Partner Extranet Module

When managed service provider (MSP) partner access is required, separate VPN connectivity to each campus building or branch location is possible but not scalable. Instead, it is recommended to centralize the VPN access from the MSP partner, providing a more maintainable and cost effective solution. In terms of the energy management solution, the primary function of the Partner Extranet Module is to provide the centralized termination of MSP partner VPN connections by which the Mediators are subsequently managed. The Partner Extranet Module also provides stateful access control of the traffic that flows through the VPN tunnels and across the enterprise network to the Mediators. Additionally, the Partner Extranet Module can be used to as an alternative means of providing Internet connectivity through which periodic logged data is exported from the Mediators to cloud services partners; either by way of proxy servers located on a partner DMZ, or through the deployment of network virtualization within the enterprise network. An example of a redundant Partner Extranet Module design is shown in Figure 8 below.

Figure 4-8 Example Redundant Partner Extranet Module Design



The following describes the numbers shown in Figure 4-8:

- **1**—ASA 5500 Security Appliances deployed within the Extranet DMZ section provides address translation and stateful access control for outgoing connections to cloud-services partners and incoming connections from managed service provider (MSP) partners through VPN devices.
- **2**—ASA 5500 Security Appliances deployed within the Extranet remote-access VPN section provides remote-access VPN termination, address translation, and IP address assignment for MSP partners.
- **3**—Cisco 1000 Series ASRs or Cisco 7200/7300 Series routers deployed within the Extranet site-to-site VPN section provides site-to-site VPN termination, stateful access control, and potentially address translation of managed services partner VPN connections.

Again, only the highlighted components that are relevant to the energy management solution are discussed in this document.

Note In Figure 4-8 above, separate IP subnets are shown connecting the routers within the service provider edge section to separate switches within the Extranet DMZ, Extranet remote-access VPN, and Extranet site-to-site VPN sections of the Partner Extranet Module. Since address translation is typically

performed within firewalls and VPN concentrators, the outside addresses of these devices are usually within the Internet routable addressing space. Since separate IP subnets normally require a larger amount of Internet routable IP addressing space to be provisioned from the service provider, enterprise organizations often combine these into a single IP subnet.

Examples of the connections that should be allowed through the ASA 5500 Series Security Appliances and/or VPN routers for energy management flows through the Partner Extranet Module are shown in Figure 4-9 and Figure 4-10.

Figure 4-9 Inbound Management Flows From MSP Partner Workstations to Mediators

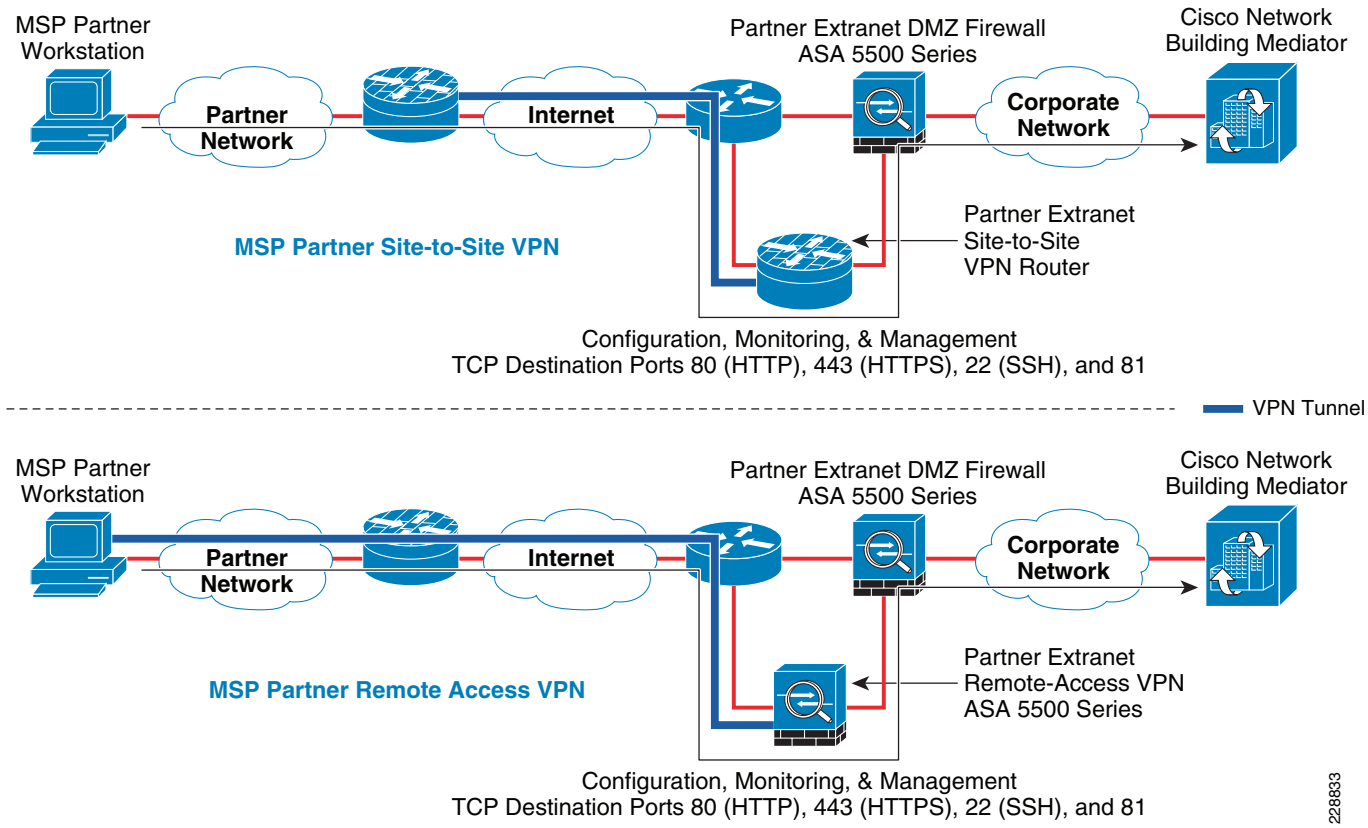


Figure 4-9 shows inbound management (configuration, monitoring, etc.) connections initiated from MSP partner workstations to the Mediators. The top half of the figure shows the flows through a site-to-site VPN tunnel, while the bottom half of the figure shows the flows through a remote-access VPN tunnel. In a site-to-site VPN configuration, the IPsec tunnel is extended from a router within the MSP partner network to a dedicated VPN router within the enterprise network. In a remote-access VPN configuration, the IPsec tunnel is extended from the MSP partner workstation to a dedicated ASA 5500 Series Security Appliance within the enterprise network. In either case, SSH (TCP port 22) is required in order for the MSP partner workstation to establish a connection to the Mediators for configuration via the ConfigTOOL application. The Omega suite of tools requires web-based access to the Mediators, either via HTTP (TCP port 80) or HTTPS (TCP port 443). Although the IPsec tunnel does protect traffic crossing the Internet between the MSP partner network and the enterprise network, the use of a secure protocol such as HTTPS can provide additional confidentiality and data integrity of the management flows as they traverse both the MSP partner network and the enterprise network. Note that the ConfigTOOL application also uses TCP port 81 to determine the state (online or offline) of the

Mediators. These protocols need to be enabled across the VPN tunnel itself; across any firewall software within the partner Extranet site-to-site VPN router or the remote-access VPN ASA 5500 Series Security Appliance; and across the partner Extranet DMZ firewall.

Figure 4-10 Data Export From Mediators to MSP Partner or Cloud Services Partner Servers via VPN

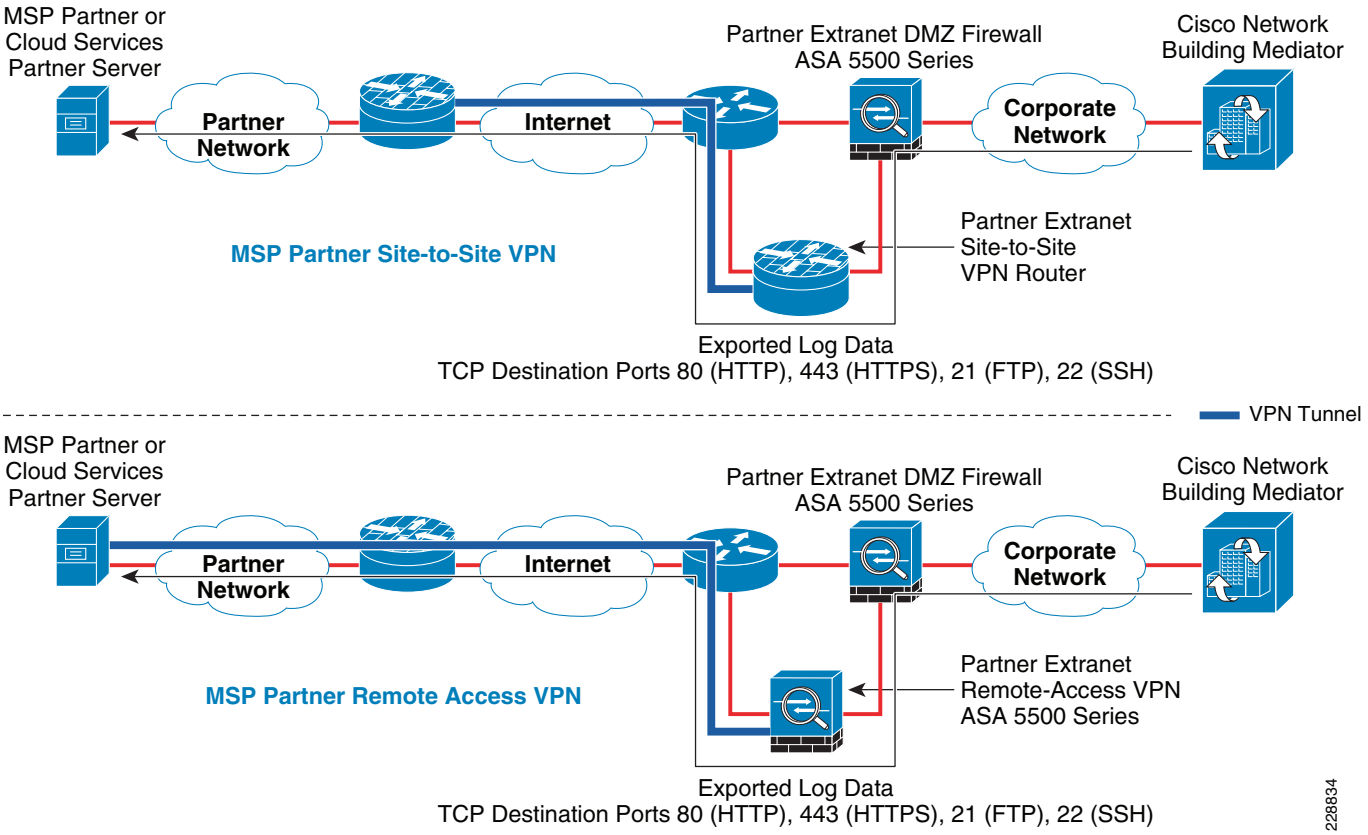


Figure 4-10 shows the export of periodic logged data initiated by the Mediators outbound toward MSP partner or cloud-services partner servers through the VPN tunnel. This scenario may be implemented when the MSP partner provides both ongoing monitoring and management of the energy management deployment, as well as providing an energy scorecard service for the enterprise customer. As discussed previously, the Mediator can periodically export logged data via HTTP, HTTPS, FTP, or Secure FTP (SSH). Typical deployments will use one of these protocols, which must be enabled across the VPN tunnel as well as through the access control of the firewalls.

When implementing a site-to-site VPN, exported log data generated from the Mediators can be used to automatically establish an IPSec tunnel, if it is not already established, with no end-user intervention. Data flows to multiple MSP partner servers (i.e., one for monitoring and management and another for energy scorecard services) is simply a matter of modifying the access-control lists that control traffic allowed across the VPN tunnels and through the various firewalls. Using a remote-access VPN for data export is somewhat more challenging. Since the Mediator cannot initiate a remote-access VPN tunnel to a MSP partner or cloud-services partner server, the remote-access VPN tunnel must already be established when the data export from the Mediator occurs. This implies the remote-access VPN tunnel is permanently established between the MSP partner or cloud-services partner server, which collects the exported log data and the enterprise network. This may require additional monitoring of the server in order to ensure the IPSec VPN tunnel is always established.

The discussion around site-to-site VPN access and remote-access VPN access in the following two sections assume a scenario in which the MSP partner is providing both ongoing monitoring and management of the Cisco Network Building Mediator deployment, as well as providing an energy scorecard service. For ease of understanding the examples, the same MSP server is providing both functions. This was done, because it demonstrates more complex site-to-site and remote-access VPN configurations. The network administrator should note that actual deployment scenarios may vary considerably. Based upon the services offered by the MSP partner, the enterprise may instead choose to export log data via the Internet (i.e., not over the VPN tunnel) to either the MSP partner or to a completely separate cloud-services partner.

Site-to-Site VPN Access

Site-to-site VPN connections are generally considered for more permanently connected requirements, meaning that a VPN tunnel is automatically established between the MSP network and the enterprise customer network based on traffic flows. This model may be useful if the MSP partner is providing ongoing monitoring and support of the energy management system, as well as collecting periodic logged data exported from the Mediators for services such as an energy scorecard. In this case, data exports initiated from the Mediators may also traverse the site-to-site VPN tunnel to the MSP partner. One advantage of this method is that the exported data and/or event data is secured by the IPSec VPN tunnel itself. Also, it is relatively easy to allow multiple MSP management workstations access through the tunnel to both manage the Mediator deployment and collect the exported data.

Site-to-site VPN connectivity can be provided with a redundant pair of Cisco 1000 Series Advanced Services Routers (ASRs), or a redundant pair of Cisco 7200 or 7300 Series routers licensed for site-to-site VPN use located within the Extranet site-to-site VPN section of the Partner Extranet Module. Example 4-2 shows an example partial configuration of a Cisco 7200 Series router (non-redundant) for site-to-site VPN connectivity.

Example 4-2 Partial Cisco 7200 Series Router Configuration for Site-to-Site VPN Access

```
!
crypto isakmp policy 10
 encr aes 256
 authentication rsa-encr
 group 2
 lifetime 180
!
!
crypto ipsec transform-set site-to-site-vpn esp-aes 256 esp-sha-hmac
!
crypto map mediator_vpn 10 ipsec-isakmp
 set peer 192.168.192.26                    ! IP address of the MSP partner VPN router.
 set transform-set site-to-site-vpn
 match address mediator_vpn_traffic         ! Controls traffic send down the VPN tunnel.
!
!
crypto key pubkey-chain rsa                 ! Public/Private key pair for authentication.
 addressed-key 192.168.192.26 encryption
  address 192.168.192.26
  key-string
   30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E06CEC
   7B9A4D57 95D52DEC 4C55A967 2B83C85B F4F21D03 CD904B6C BECC7BB6 310115D1
   D634B04C A35F1294 886C2F40 FFEDEB34 9C515DC3 B5B7CCE5 C3E46286 950F6E30
   1983A3AE D5B03FD5 3A280657 48283817 E5384686 06DE82E9 6D49A17F 79277FAC
   C9B28AA1 55063C2E CA9F6DA1 831E7389 11FDAD02 F3A9FED7 3D83ED04 9B020301 0001
  quit
```

```
!
~
!
class-map type inspect match-all vpn-inside-tcp-81-cmap
 match access-group name mediator_mgmt_tcp_81
class-map type inspect match-all inside-vpn-ftp-cmap
 match protocol ftp
 match access-group name mediator_export_ftp_ssh_http_https
class-map type inspect match-all inside-vpn-https-cmap
 match protocol https
 match access-group name mediator_export_ftp_ssh_http_https
class-map type inspect match-all vpn-inside-https-cmap
 match protocol https
 match access-group name mediator_mgmt_web_ssh
class-map type inspect match-all inside-vpn-ssh-cmap
 match protocol ssh
 match access-group name mediator_export_ftp_ssh_http_https
class-map type inspect match-all vpn-inside-ssh-cmap
 match protocol ssh
 match access-group name mediator_mgmt_web_ssh
class-map type inspect match-ll vpn-inside-8443-cmap
 match access-group name mediator_export_https
class-map type inspect match-all inside-vpn-http-cmap
 match protocol http
 match access-group name mediator_export_ftp_ssh_http_https
class-map type inspect match-all vpn-inside-http-cmap
 match protocol http
 match access-group name mediator_mgmt_web_ssh
!
!
policy-map type inspect inside-outside-pmap  ! Policy map to inspect inside traffic going
                                             ! out the VPN tunnel.
 class type inspect inside-vpn-http-cmap
  inspect
 class type inspect inside-vpn-https-cmap
  inspect
 class type inspect inside-vpn-ftp-cmap
  inspect
 class type inspect inside-vpn-ssh-cmap
  inspect
 class type inspect vpn-inside-8443-cmap
  inspect
 class class-default
  drop
policy-map type inspect outside-inside-pmap ! Policy map to inspect VPN traffic coming in
                                              ! form the VPN tunnel.
 class type inspect vpn-inside-http-cmap
  inspect
 class type inspect vpn-inside-https-cmap
  inspect
 class type inspect vpn-inside-ssh-cmap
  inspect
 class type inspect vpn-inside-tcp-81-cmap
  inspect
 class class-default
  drop
!
zone security outside
zone security inside
zone-pair security inside-outside source inside destination outside
 service-policy type inspect inside-outside-pmap
zone-pair security outside-inside source outside destination inside
 service-policy type inspect outside-inside-pmap
!
```

```
~
!
interface GigabitEthernet0/1
 description CONNECTION TO INTERNET (VPN OUTSIDE INTERFACE)
 ip address 10.192.181.5 255.255.255.248
 ip access-group vpn_tunnel_establishment in ! Controls Internet traffic to the VPN
                                            ! router.
 zone-member security outside                ! Firewall outside zone.
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
 crypto map mediator_vpn                     ! VPN tunnel originates from this interface.
!
interface GigabitEthernet0/2
 description CONNECTION TO ME-EASTFIRE-1 (VPN INSIDE)
 ip address 10.16.4.4 255.255.255.0
 zone-member security inside                 ! Firewall inside zone.
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
!
~
!
ip route 10.192.2.0 255.255.255.0 10.192.181.1       ! Static route pointing to the
                                                     ! partner network.
ip route 192.168.192.24 255.255.255.252 10.192.181.1 ! Static route pointing to the
                                       ! Internet facing side of the partner VPN router.
!
~
!
ip access-list extended mediator_export_ftp_ssh_http_https
 remark Allow Mediator to Export hourly reports
 permit ip host 10.16.4.50 host 10.192.2.3
ip access-list extended mediator_export_https
 remark Allow Mediator to Export hourly reports via HTTPS
 permit tcp host 10.16.4.50 host 10.192.2.3 eq 8443
ip access-list extended mediator_mgmt_tcp_81
 remark Allow TCP 81 from partner mgmt workstations to Mediator NAT
 permit tcp host 10.192.2.3 host 10.16.4.50 eq 81
ip access-list extended mediator_mgmt_web_ssh
 remark Allow partner mgmt workstations to Mediator NAT
 permit ip host 10.192.2.3 host 10.16.4.50
ip access-list extended mediator_vpn_traffic
 remark Allow Mediator NAT to MSP managemet workstation
 permit ip host 10.16.4.50 host 10.192.2.3
ip access-list extended vpn_tunnel_establishment
 remark Allow S2S VPN from partner router
 permit esp host 192.168.192.26 host 10.192.181.5
 permit udp host 192.168.192.26 eq isakmp host 10.192.181.5
!
```

Typical site-to-site VPN connectivity uses IPSec, with AES 128-bit or higher encryption for data confidentiality and integrity. The IPSec crypto map in the example above uses AES encryption with a 256-bit key, and HMAC-SHA1 for data authentication. The crypto map also shows a self-generated public-private RSA key pair for IKE authentication. This is somewhat more secure than a shared secret, since the MSP partner VPN router must possess the private key in order to authenticate to the enterprise VPN router; without having to deploy a full public-key infrastructure (PKI) system.

Note that a classic VPN tunnel was selected for the example, as opposed to the use of virtual tunnel interface (VTI) for the VPN tunnel. Therefore, in this example, the VPN tunnel endpoint is the Internet-facing interface of the VPN router (GigabitEthernet0/1). It is recommended that the configuration should be as specific as possible, in terms of allowing access from individual MSP partner management workstations to individual Mediators (or a hierarchical mediator or Mediator Manager within the enterprise network which then allows access to individual Mediators), within the crypto ACL which controls traffic across the VPN tunnel. Access control should be specified at least down to the host level. In the example above, the access-list named "mediator_vpn_traffic" allows only traffic from IP host 10.16.4.50 to IP host 10.192.2.3 to go down the VPN tunnel. Overlapping IP address spaces between the enterprise network and the MSP partner network may often complicate site-to-site VPN deployments, requiring the deployment of NAT. IP address 10.16.4.50 is a NATed IP address of the actual Mediator sitting within the enterprise network. The NAT function could be done at the VPN router. However, for this design example NAT is done at the ASA 5500 firewall within the Extranet DMZ section of the Partner Extranet module. The crypto ACL of the VPN router could be specified down to the protocol level to allow only HTTP, HTTPS, FTP, and/or SSH traffic between the partner management workstations and individual Mediators. However, as will be discussed shortly, both the Zone-Based Policy Firewall (ZBPF) on the VPN router as well as the ASA 5500 firewall policy already restrict access down to the protocol level.

It is recommended that no active IP routing protocols be in operation between the MSP partner network and the enterprise network where possible. Instead, IP routes can be statically defined and redistributed to active routing protocols within each network. These should be restricted to only those routes necessary for the establishment of the VPN tunnel and for the partner management host subnet to reach the Mediator subnet. Note that these subnets may correspond to DMZ subnets on both the enterprise and MSP partner sides due to the use of NAT. This hides the true IP addressing of the enterprise and MSP partner networks, and simplifies the issue of overlapping IP addressing space in both the MSP partner and enterprise networks.

Access control of inbound Internet traffic to the VPN router, as well as unencrypted MSP partner traffic, can be accomplished multiple ways. Basic ACLs can be configured to restrict inbound traffic from the Internet facing interface to only IPSec and ISAKMP protocols, as is shown in the example. Technically, this may be somewhat redundant, since ZBPF is also enabled on the VPN router, and no policy exists that allows non-VPN Internet traffic from the outside security zone to the inside security zone of the VPN router. Likewise basic ACLs could be configured to restrict inbound traffic from the inside-facing interface to allow only the Mediator hosts to communicate to the MSP partner hosts. These could be specified down to the protocol level. Keep in mind, however, that FTP uses a dynamic port range for data transfer. If configuring an ACL down to the protocol level, and if FTP data export is supported over the VPN tunnel, then a range of ports may need to be opened to support the FTP exports from the Mediators. Alternatively, access control can be accomplished via ZBPF functionality on Cisco 1000 Series Advanced Services Router (ASR); or via either ZBPF functionality or Context-Based Access Control (CBAC) functionality on Cisco 7200 and 7300 Series routers.

In the example above, ZBPF functionality is enabled on the Cisco 7200 Series router, with two security zones established. The Internet-facing interface of the VPN router (GigabitEthernet0/1) is part of the outside security zone. Note that, since the VPN tunnel is established from this interface, the VPN tunnel is part of the outside security zone. The inside interface of the VPN router (GigabitEthernet0/2) is part of the inside security zone. The "inside-outside-pmap" policy map allows HTTP, HTTPS, FTP, and SSH protocols from the NATed IP address of the Mediator to the IP address of the MSP partner workstation. The "outside-inside-pmap policy" allows HTTP, HTTPS,SSH, and TCP port 81 from the IP address of the MSP partner host—reachable via the VPN tunnel—to the NATed IP address of the Mediator. These are protocols necessary for data export from the Mediator to the MSP partner server, as well as inbound management from the MSP partner server, respectively. In real deployments, a subset of protocols may be implemented, depending upon the requirements of the MSP partner. For example, the MSP partner may utilize separate IP hosts, both visible over the VPN tunnel for data export and for management. Alternatively, the data export may be sent to a separate cloud services partner on the Internet, reachable

via the ASA 5500 firewall in the Extranet DMZ section of the Partner Extranet Module. In this case, the zone-based policy firewall running on the VPN router may be configured not to allow any inbound traffic initiated from the Mediator. Finally, note that the default class within each policy map indicates that all other traffic should be dropped. The functioning of the zone-based policy firewall can be verified with the **show policy-map type inspect zone-pair** command.

Note TCP port 8443 was added in the example above to verify HTTPS functionality during the testing of the design, since the Apache Tomcat server defaults to port 8443 for HTTPS.

Besides the use of zone-based policy firewall on the VPN router, another alternative is to send the unencrypted MSP partner traffic from the site-to-site VPN router to a DMZ interface off the ASA 5500 firewall within the Extranet DMZ section of the Partner Extranet Module, as was shown in Figure 4-6 on page 4-7. This design option is in alignment with the security concept of "defense-in-depth". Alternatively, providing the stateful firewalling function within a dedicated ASA 5500 firewall and simply using ACLs on the VPN router can reduce the CPU utilization of the VPN router for additional scalability. In either case, besides a second layer of access control, this has the additional advantage in that NAT can be done at the ASA 5500 firewall, hiding the true IP addressing of the Mediators. All of the Mediators within an enterprise network appear as a series of statically NATed IP addresses off a DMZ segment within the Partner Extranet Module in this design. A partial configuration (non-redundant) from the ASA 5500 firewall for this type of design is shown in Example 4-3.

Example 4-3 Partial Configuration from the Extranet DMZ ASA 5500 Firewall

```
names
name 10.192.2.3 vc_a2_internet description Internet Address of VC-A2      ! MSP Partner
Host
name 10.16.4.50 me-westcampus-mediator-nat description NATed addresss of mediator for S2S
VPN
name 10.17.192.2 me-westcampus-mediator description West Campus Mediator
!
~
!
interface GigabitEthernet0/2
 description me-eastfire-3 g1/0/17 vlan 51
 nameif dmz
 security-level 50
 ip address 10.16.4.1 255.255.255.0
!
interface GigabitEthernet1/0
 description me-eastdist-1 g5/25 vrf bin
 nameif inside_bin
 security-level 75
 ip address 10.16.19.193 255.255.255.252
!
~
!
object-group service DM_INLINE_TCP_6 tcp     ! Inbound SSH, HTTP, & HTTPS
 port-object eq ssh
 group-object web
 port-object eq 81
object-group service DM_INLINE_TCP_3 tcp     ! Outbound FTP, SSH, HTTP, & HTTPS
 port-object eq 8443
 port-object eq ftp
 port-object eq ssh
 group-object web
object-group service web tcp
 port-object eq www
 port-object eq https
```

```
object-group network Mediators
 description Cisco Network Building Mediators
 network-object host me-westcampus-mediator
!
~
!
access-list dmz_access_in remark Allow management server access to NATed address of
Mediators.
access-list dmz_access_in extended permit tcp host vc_a2_internet host
me-westcampus-mediator-nat object-group DM_INLINE_TCP_6
access-list inside_bin_access_in remark Allow Data Export from Mediators to VC-A2 via
site-to-site VPN
access-list inside_bin_access_in extended permit tcp object-group Mediators host
vc_a2_internet object-group DM_INLINE_TCP_3
!
~
!
static (inside_bin,dmz) me-westcampus-mediator-nat me-westcampus-mediator netmask
255.255.255.255
!                                          ! Static NAT
!
~
!
access-group dmz_access_in in interface dmz
access-group inside_bin_access_in in interface inside_bin
!
~
!
route dmz 10.192.2.0 255.255.255.0 10.16.4.4 1
route inside_bin 10.17.192.0 255.255.255.248 10.16.19.194 1
!
~
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp                               ! Application-layer inspection of FTP traffic
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect http
  inspect dns
!
service-policy global_policy global
!
```

Access control configured on the ASA 5500 firewall again allows only HTTP, HTTPS, SSH, and TCP port 81 traffic from the MSP partner host to access the Mediator via the statically NATed IP address. Likewise, only HTTP, HTTPS, SSH, and FTP traffic are allowed from the Mediator to the MSP partner host. Note that TCP port 8443 was allowed to validate HTTPS functionality since Apache Tomcat defaults to TCP port 8443 for HTTPS. This provides a second line of access control on top of VPN

router, as well as a single point of entry for partner data flows into the enterprise network. Since partner connectivity requirements are typically much more well-defined than general employee access to the Internet, the Extranet DMZ firewall may be locked down much tighter with both inbound and outbound access control, versus allowing all connectivity outbound, as is often done with the Internet Edge Module firewall. This is another advantage of deploying a separate firewall within a Partner Extranet Module. Finally, note that application-layer inspection on the ASA 5500 firewall will dynamically open the port range needed for FTP transfers, versus opening a range of ports on a static ACL.

Remote-Access VPN Access

Remote-access VPN connections are generally considered for more temporarily connected requirements, although such VPN connections may be left up for extended periods of time as well, based on the particular business requirements of the energy management solution. With remote-access VPN connectivity, individual MSP partner workstations establish tunnels to a VPN concentrator in order to manage the Mediator deployment. If exporting of logged data is done through remote-access VPN connectivity, individual MSP partner or cloud service partner servers also need to establish tunnels to a VPN concentrator in order to provide a path for the data export from the Mediators to reach them.

Remote-access VPN connectivity can be provided with a redundant pair of ASA 5500 Series Security Appliances licensed for remote-access VPN use deployed within the Extranet remote-access VPN section of the Partner Extranet Module. Typical MSP remote-access VPN connections also uses IPSec with AES 128-bit or higher encryption for data confidentiality and integrity. This may require client software, such as the Cisco VPN Client, to be deployed on the MSP partner and/or cloud services partner workstations and servers. Example 4-4 shows a partial example configuration (non-redundant) of an ASA 5500 for remote-access VPN connectivity.

Example 4-4 Example of a Partial ASA 5500 Series Configuration for Remote-Access VPN Connectivity

```
!
names
name 10.192.181.6 user_inet description Firewall Outside Internet Interface
name 10.17.192.2 me-westcampus-mediator description West Campus Mediator
name 10.17.2.10 me-westserv-2 description Radius Server
name 10.16.19.2 vc-a2-vpn_alternate description MSP partner Server RAVPN IP Address
name 10.16.19.193 inside_bin_interface description Firewall Building Information Network
Interface
!
interface GigabitEthernet0/3
 description OC3 Internet Access via me-eastinet-3 & 4
 nameif outside
 security-level 25
 ip address user_inet 255.255.255.248
!
interface GigabitEthernet1/0
 description BIN VRF via me-eastdist-1 g5/25
 nameif inside_bin
 security-level 75
 ip address inside_bin_interface 255.255.255.252
!
!
object-group service web tcp
 port-object eq www
 port-object eq https
!
object-group network Mediators
 description Cisco Network Building Mediators
 network-object host me-westcampus-mediator
```

```
!
object-group service DM_INLINE_TCP_5 tcp
 port-object eq 8443
 port-object eq ftp
 port-object eq ssh
 group-object web
object-group service DM_INLINE_TCP_7 tcp
 port-object eq 8443
 port-object eq ftp
 port-object eq ssh
 group-object web
object-group service DM_INLINE_TCP_8 tcp
 port-object eq 8443
 port-object eq ftp
 port-object eq ssh
 group-object web
object-group service DM_INLINE_TCP_10 tcp
 port-object eq ftp
 port-object eq ssh
 group-object web
 port-object eq 81
object-group service DM_INLINE_TCP_11 tcp
 port-object eq ftp
 port-object eq ssh
 group-object web
 port-object eq 81
object-group network msp-ravpn-server-group
 description MSP mgmt workstation group visible via RAVPN
 network-object host vc-a2-vpn_alternate
!
access-list remote_access_user extended permit tcp object-group msp-ravpn-server-group
object-group DM_INLINE_TCP_8 object-group Mediators
access-list remote_access_user extended permit tcp object-group msp-ravpn-server-group
object-group Mediators object-group DM_INLINE_TCP_11
!
access-list remote_access_group extended permit tcp object-group msp-ravpn-server-group
object-group DM_INLINE_TCP_5 object-group Mediators
access-list remote_access_group extended permit tcp object-group msp-ravpn-server-group
object-group Mediators object-group DM_INLINE_TCP_10
!
access-list inside_bin_access_in remark Allow Data Export from Mediators to VC-A2 via
remote-access VPN
access-list inside_bin_access_in extended permit tcp object-group Mediators object-group
msp-ravpn-server-group object-group DM_INLINE_TCP_7
!
access-list inside_bin_nat0_outbound remark Allow Mediators to reach assigned IP address
for RA VPN.
access-list inside_bin_nat0_outbound extended permit ip object-group Mediators
object-group msp-ravpn-server-group
!
access-list me-nets remark east coast
access-list me-nets standard permit 10.16.0.0 255.255.0.0
access-list me-nets remark west coast
access-list me-nets standard permit 10.17.0.0 255.255.0.0
!
access-list splitTunFWIn remark Roland's office
access-list splitTunFWIn extended permit ip 64.100.160.0 255.255.255.0 any
!
ip local pool mediator_vpn 10.16.19.4-10.16.19.14 mask 255.255.255.240
!                                        ! IP address pool (not used in this example)
!
nat-control
nat (inside_bin) 0 access-list inside_bin_nat0_outbound
```

```
!                                              !Don't NAT access to the assigned address of
the RA VPN devices
nat (inside_bin) 1 0.0.0.0 0.0.0.0
!
access-group inside_bin_access_in in interface inside_bin
!                                              ! Allow Mediator export to RA VPN devices
using
!                                              ! SSH, FTP, and HTTPS
!
route outside 0.0.0.0 0.0.0.0 10.192.181.1 1
route inside_bin 10.17.192.0 255.255.255.248 10.16.19.194 1
!
dynamic-access-policy-record IPsec_RAVPN_Dynamic_Policy
 description "Dynamic Access Policy for RAVPN Clients"
 network-acl remote_access_user              ! Specifies per-user RA VPN access control
!
aaa-server radius-server protocol radius     ! Specifies the RADIUS server
aaa-server radius-server (inside) host me-westserv-2
 key ciscoese
 authentication-port 1812
 accounting-port 1813
 radius-common-pw ciscoese
!
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto ipsec df-bit clear-df inside
crypto ipsec df-bit clear-df mgmt
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-AES-128-SHA
ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5
ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set security-association lifetime
seconds 28800
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set security-association lifetime
kilobytes 4608000
crypto map user_inet_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map user_inet_map interface outside  ! Crypto map applied to the outside interface
crypto isakmp enable outside                ! IKE enabled on outside interface
crypto isakmp policy 5
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!
group-policy DfltGrpPolicy attributes      ! Default RA VPN policy group
 banner value Unauthorized Access is Prohibited.
 vpn-filter value remote_access_group      ! Defines access control at the group level
 vpn-tunnel-protocol IPSec webvpn
```

```
 ipsec-udp enable
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value me-nets   ! Defines ACL for split tunneling at the client
 secure-unit-authentication enable
 user-authentication enable
 address-pools value mediator_vpn          ! Assigns IP address pool to the default group
policy
 client-firewall opt cisco-integrated acl-in splitTunFWIn acl-out open
!                                          !Defines client firewall ACL at the client
 webvpn
  url-list value Mediator
  svc compression none
  svc ask none default webvpn
  http-comp none
  smart-tunnel enable Mediator_Configuration
  url-entry disable
!
group-policy IPsec_VPN_Group_Policy_2 internal
!                                          ! RA VPN policy group using RADIUS user
authentication
group-policy IPsec_VPN_Group_Policy_2 attributes
 vpn-tunnel-protocol IPSec                 ! Allows only IPsec VPN
 group-lock value vc-a2-acs2
 address-pools none                        ! Overrides default group policy use of IP
address pool
!
group-policy IPsec_VPN_Group_Policy internal
           ! RA VPN policy group using local userid authentication
group-policy IPsec_VPN_Group_Policy attributes
 vpn-tunnel-protocol IPSec                 ! Allows only IPsec VPN
 group-lock value vc-a2
 address-pools none                        ! Overrides default group policy use of IP
address pool
!
username joeuser1 password aSnrkw/Y3WIwmRvT encrypted
!                                          ! Local userid definition (note that the userid
is the same as
username joeuser1 attributes               ! the IPsec connection profile in this example
configuration)
 vpn-group-policy IPsec_VPN_Group_Policy
 vpn-framed-ip-address 10.16.19.2 255.255.255.240
           ! Local assignment of IP address specific to userid
 service-type remote-access
!
tunnel-group vc-a2 type remote-access     ! IPsec connection profile for local
authentication
tunnel-group vc-a2 general-attributes
 authorization-server-group LOCAL
 default-group-policy IPsec_VPN_Group_Policy
tunnel-group vc-a2 ipsec-attributes
 pre-shared-key *
!
tunnel-group vc-a2-acs2 type remote-access ! RA VPN policy group using RADIUS
authentication
tunnel-group vc-a2-acs2 general-attributes
 authentication-server-group radius-server
 authorization-server-group radius-server
 default-group-policy IPsec_VPN_Group_Policy_2
tunnel-group vc-a2-acs2 ipsec-attributes
 pre-shared-key *
!
```

One advantage of remote-access VPN connectivity is that access control can be provisioned on a per group and/or per user basis. The configuration in Example 4-4 above shows two different remote access VPN group policies called “IPsec_VPN_Group_Policy” and “IPsec_VPN_Group_Policy2”, for illustrative purposes. Both group policies inherit some attributes from the default VPN group policy named “DfltGrpPolicy”, and also override other attributes. This hierarchical grouping allows the network administrator to define the default policy more generically, and then restrict further with policies specific to individual groups, such as a group policy specifically defined for MSP partner remote access VPN connections. In the configuration above, the default VPN group policy specifies the access-control list named “remote_access_group” as a group level filter. Both VPN group policies shown in the configuration above utilize this filter. However, both VPN group policies shown in the configuration above override their VPN tunnel protocols to use only IPSec, instead of IPSec and SSL. Likewise, both VPN group policies override the assignment of the IP address of the client. Instead of using IP address from the pool “mediator_vpn”, the IP address for the groups is assigned per user.

The Cisco Network Building Mediator periodically exports logged data to a destination based either on a hostname or an IP address. There are some inherent delays in propagating dynamic DNS updates around a large enterprise network, as well as potential issues regarding the caching of DNS entries within the Mediator itself. For this reason, if the periodic export of logged data from the Mediators is through a remote-access VPN connection, then a static IP address should be handed to the MSP partner or cloud services partner server when it establishes the remote-access VPN tunnel. Identification of the server can be done based upon the userid when the remote-access VPN tunnel is established. In other words, the assignment of the IP address can be based upon the userid. An example has been provided regarding how the IP address is specified per userid. Within the configuration in Example 4-4 above, the IPSec connection profile (tunnel-goup) called “vc-a2” has been defined to use the policy group named “IPsec_VPN_Group_Policy”. Tunnel-group “vc-a2” specifies the use of the local database for authentication of individual users. A userid of “joeuser1” has also been defined within the configuration example. Under the attributes of the username, the **vpn-framed-ip-address** command is used to statically assign an IP address to the particular userid.

However, the configuration of userids directly on the ASA 5500 Series Security Appliance is generally not considered a best practice. For any sizeable enterprise deployment, a best practice is to handle the access control decision centrally through a AAA server connected to the ASA 5500 Series Security Appliance via either the RADIUS or TACACS+ protocol. The AAA server may in turn be connect to a backend directory server. An example of a AAA server is the Cisco Secure Access Control Server (ACS), which can be deployed either within a Data Center or Campus Service Module within the campus network. Centralized control allows the network administrator to more effectively maintain the list of partner userids who have access to the enterprise network. It also allows the network administrator to add or remove partner userids quickly, without having to potentially touch multiple local databases in multiple network devices. It is essential that network administrator work closely with the MSP partner to immediately identify any employees who leave the company, so that their access to the enterprise network can be immediately revoked. Alternatives to the use of individual passwords include the use of token cards or token software installed on the MSP partner workstation. This requires the MSP employee either to have physical access to the PC or physical access to the token card in order to access the enterprise network. Within the configuration in Example 4-4, a second IPSec connection profile (tunnel-group) called “vc-a2-acs” has been defined to use the policy group named “IPsec_VPN_Group_Policy2”. Tunnel-group “vc-a2-acs” specifies the use of a RADIUS server group for authentication of individual users. Within the RADIUS server itself, specific userids are defined. The *Framed-IP-Address* and *Framed-IP-Netmask* RADIUS attributes defined for each userid can be used in order to return a specific IP address, based upon the particular userid. Per-user filtering can be accomplished through the application of a dynamic access policy which is configured to key in on a specific AAA attribute such as the userid. In the configuration above, the access-list named “remote_access_group” is used applied based on userid.

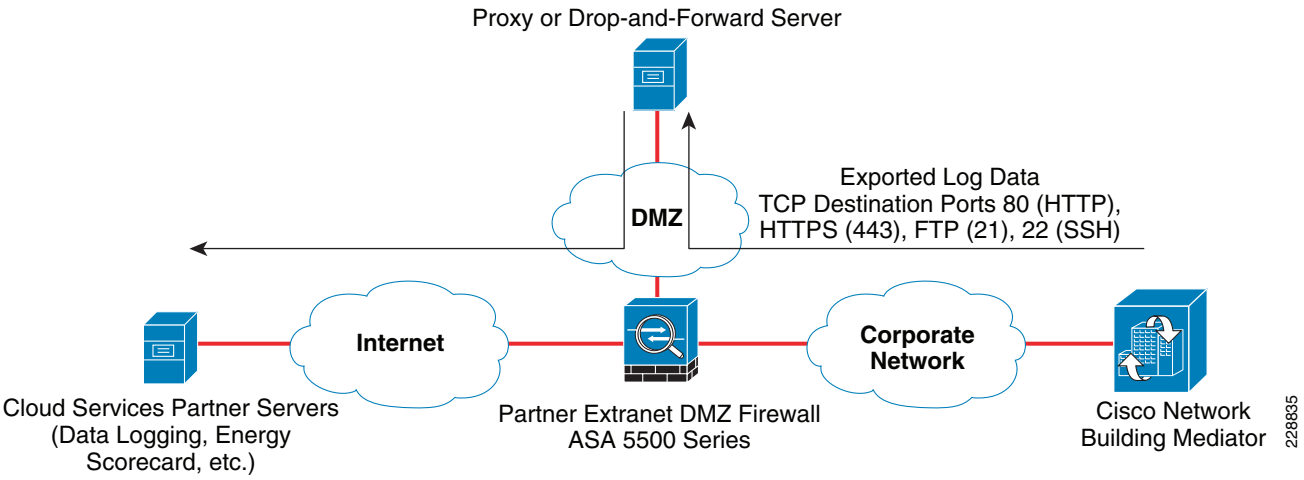
The network administrator should take note that, if the export of periodic logged data from the Mediator does not use the remote-access VPN tunnel, then assignment of IP addresses to MSP partner VPN clients can be based on an address pool. In such cases, the access-control lists need to be modified to allow for the required protocols across the range of IP addresses. Finally, as with site-to-site VPN connections, the MSP data flows which terminate on the remote-access VPN ASA 5500s can also be routed to a separate segment off of the Extranet DMZ firewalls, as shown in Figure 4-8 on page 4-10. This provides a second layer of access control and provides a single point of entry for partner traffic into the enterprise network.

Note The use of SSL VPN technology to access the Cisco Network Building Mediator has not been thoroughly tested by ESE as of the time this document was written; and has therefore not been validated to work entirely correctly.

Internet Access for Exporting of Logged Data

As mentioned previously, the Extranet Module can be used to as an alternative means of providing Internet connectivity through which data is exported from the Mediators to cloud services partners. The first method of doing so is through the use of secure proxy or drop-and-forward servers located on the Extranet DMZ section of the Extranet Module. An example of this is shown in Figure 4-11.

Figure 4-11 Example Proxy Server Deployment for Mediator Log File Export via the Extranet Module



Note that Figure 4-11 is nearly identical to Figure 4-4. The only difference is that the Mediator exported logged-data passes through a secure proxy or drop-and-forward server located within the Extranet DMZ section of the Partner Extranet Module. The Partner Extranet DMZ firewall shown in Figure 4-11 is a firewall dedicated for partner traffic, separate from the firewall dedicated employee traffic deployed within the Internet Edge module. Typically, the default route for the overall enterprise network out to the Internet—therefore, to cloud-services partner servers which are reachable via the Internet—is through the Internet edge firewall. However, as discussed previously, the Mediator can be configured to use a proxy server in order to export log files via protocols such as FTP. In such cases, the Mediator only needs to be able to route to the IP address of the proxy server. The proxy server then uses a separate default route to the Internet via the Extranet DMZ firewall.

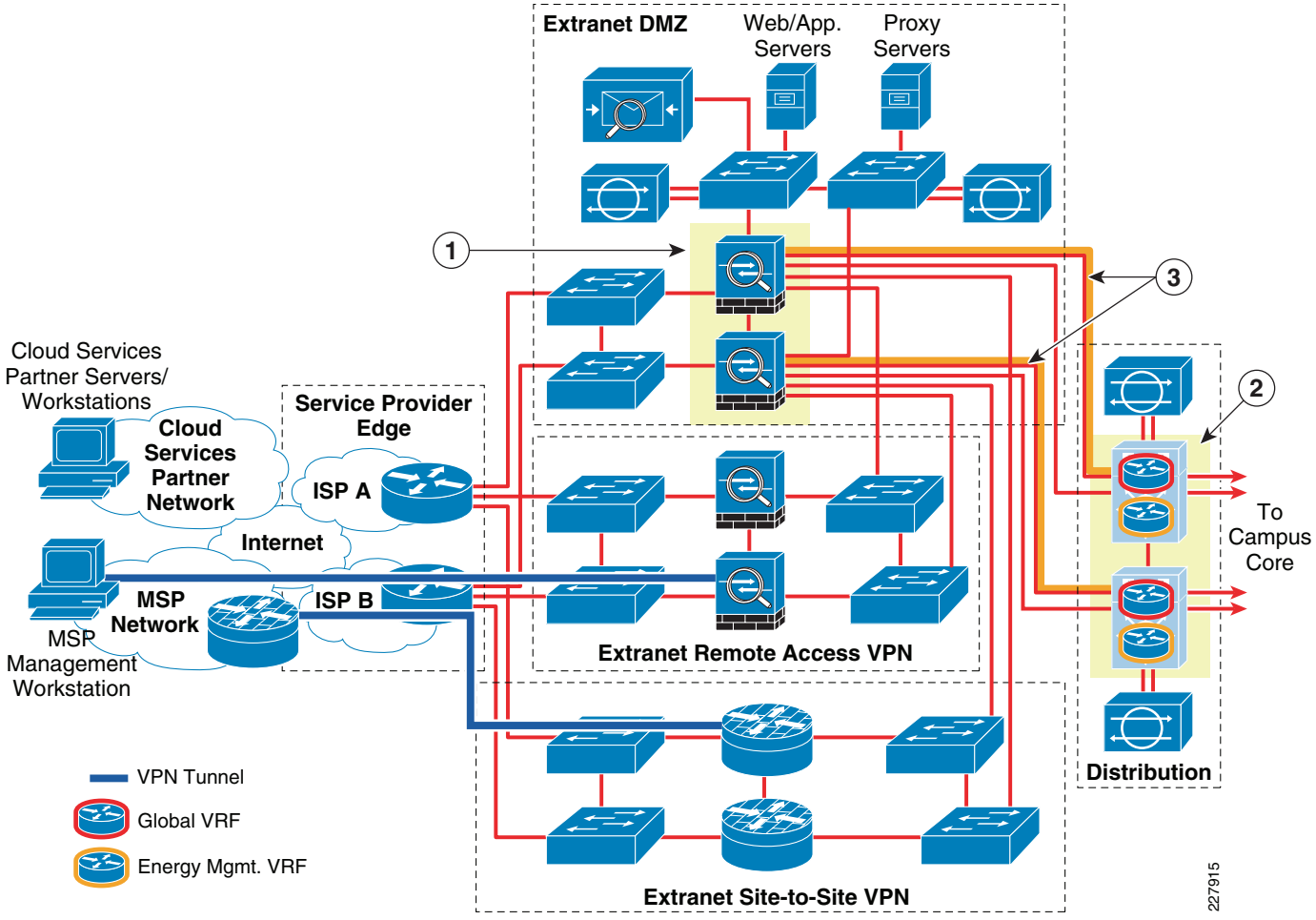
Again, the benefit of using a proxy or drop-and-forward server is that it decouples the sessions between the Mediators and the DMZ server from the sessions between the cloud services partner servers and the DMZ server. It should be noted, however, that the use of either a proxy or a drop-and-forward server adds additional administrative overhead and another possible point of failure. Therefore the additional security gained from such implementations should be weighed against the administrative overhead incurred.

A second method of using the Extranet Module as an alternative means of providing Internet connectivity through which data is exported from the Mediators to cloud services partners is through the use of virtual routing and forwarding (VRF) technology. This is discussed further in the next section.

Extending VRFs to the Partner Extranet Module

When deploying network virtualization for the energy management solution, the VRF which supports the Mediators needs to be extended through the Campus Module out to the Partner Extranet Module. Figure 4-12 shows a modified version of the Partner Extranet Module which supports virtualization for the energy management solution.

Figure 4-12 Example Redundant Partner Extranet Module Design with VRFs



The following describes the numbers in Figure 4-12:

- **1**—ASA 5500 Security Appliances deployed within the Extranet DMZ section provides address translation and stateful access control for outgoing connections to cloud-services partners and incoming connections from MSP partners through VPN devices.
- **2**—ASA 5500 Security Appliances deployed within the Extranet remote-access VPN section provides remote-access VPN termination, address translation, and IP address assignment for MSP partners.
- **3**—Cisco 1000 Series ASRs or Cisco 7200/7300 Series routers deployed within the Extranet site-to-site VPN section provides site-to-site VPN termination, stateful access control, and potentially address translation of managed services partner VPN connections.
- **4**—Traffic destined for the energy management VRF is routed to separate interfaces on the Extranet DMZ Firewalls.

In this example, the Catalyst 6500 switches within the distribution section of the Partner Extranet Module are configured to support a separate virtual routing and forwarding (VRF) instance for the energy management solution. This is then mapped to GRE tunnels which extend the energy management solution VRF back to either a Campus Service Module or Data Center Service Module. From there, other GRE tunnels extend out to campus buildings or branch locations which house the individual Mediators. This provides a star configuration, versus provisioning separate GRE tunnels from the Partner Extranet Module to each location which houses a Mediator. Note that this configuration also facilitates a hierarchical Mediator deployment, where access to the remote mediators is accomplished via a hierarchical Mediator (or future Mediator Manager appliance) located within a Campus Service Module or Datacenter Service Module. A partial configuration example of a Catalyst 6500 switch within the Distribution section of the Partner Extranet Module is shown in Example 4-5.

Example 4-5 Partial Configuration Example of VRFs Extended to the Partner Extranet Module

```
!
ip vrf bin                                    ! Configures the Building Information Network
(BIN) VRF.
rd 251:127
!
~
!
interface Tunnel0                             ! GRE tunnel to the Datacenter Module for the
BIN VRF.
 description VRF FOR MEDIATOR NETWORK TO ME-W-DCSERV-1
 ip vrf forwarding bin
 ip address 10.17.192.42 255.255.255.248
 tunnel source Loopback0
 tunnel destination 10.17.252.2
!
interface Loopback0
 ip address 10.16.255.40 255.255.255.255
!
interface Loopback2
 description LOOPBACK INTERFACE FOR TUNNEL TO ME-W-DCSERV-1
 ip vrf forwarding bin
 ip address 10.16.255.40 255.255.255.255
!
~
!
interface GigabitEthernet1/25
! Interface which connects to the ASA 5500 firewall.
 description ASA5550 G1/0 mediator vpn
 switchport
 switchport access vlan 192
 switchport mode access
 load-interval 30
```

```
 wrr-queue bandwidth 5 25 40
 priority-queue queue-limit 30
 wrr-queue queue-limit 5 25 40
 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 60 70 80 90 100 100 100 100
 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 max-threshold 3 70 80 90 100 100 100 100 100
 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 3 2 3
 wrr-queue cos-map 3 3 6
 wrr-queue cos-map 3 4 7
 priority-queue cos-map 1 4 5
 mls qos trust dscp
!
~
!
interface Vlan192
! SVI for the BIN VRF is part of an HSRP group
 ip vrf forwarding bin
! for high availability.
 ip address 10.16.19.195 255.255.255.240
 standby 192 ip 10.16.19.194
 standby 192 priority 110
 standby 192 track GigabitEthernet1/25 20
!
~
!
router eigrp 110
 network 10.16.0.0 0.0.255.255
 eigrp router-id 10.16.255.21
 no auto-summary
 passive-interface default
 no passive-interface GigabitEthernet1/1
 no passive-interface GigabitEthernet1/46
 no passive-interface GigabitEthernet3/0/0
 no passive-interface GigabitEthernet3/0/1
 no passive-interface TenGigabitEthernet6/1
 no passive-interface TenGigabitEthernet6/2
 redistribute static metric 1000000 100 255 1 1500 route-map FW_route_inject
 redistribute bgp 64000 metric 100000 150 255 1 15000
 !
 address-family ipv4 vrf bin                ! EIGRP autonomous system 99 provides routing
for
  autonomous-system 99                       ! the BIN VRF.
  network 10.16.19.0 0.0.0.255
  network 10.16.255.0 0.0.0.255
  network 10.17.192.0 0.0.0.255
  no auto-summary
  passive-interface Vlan192
  passive-interface Loopback2
  redistribute static metric 12100 250 255 1 1500
 exit-address-family
!
ip route vrf bin 0.0.0.0 0.0.0.0 10.16.19.193  ! Static default route for the
!                                               ! BIN VRF points to the ASA firewall.
```

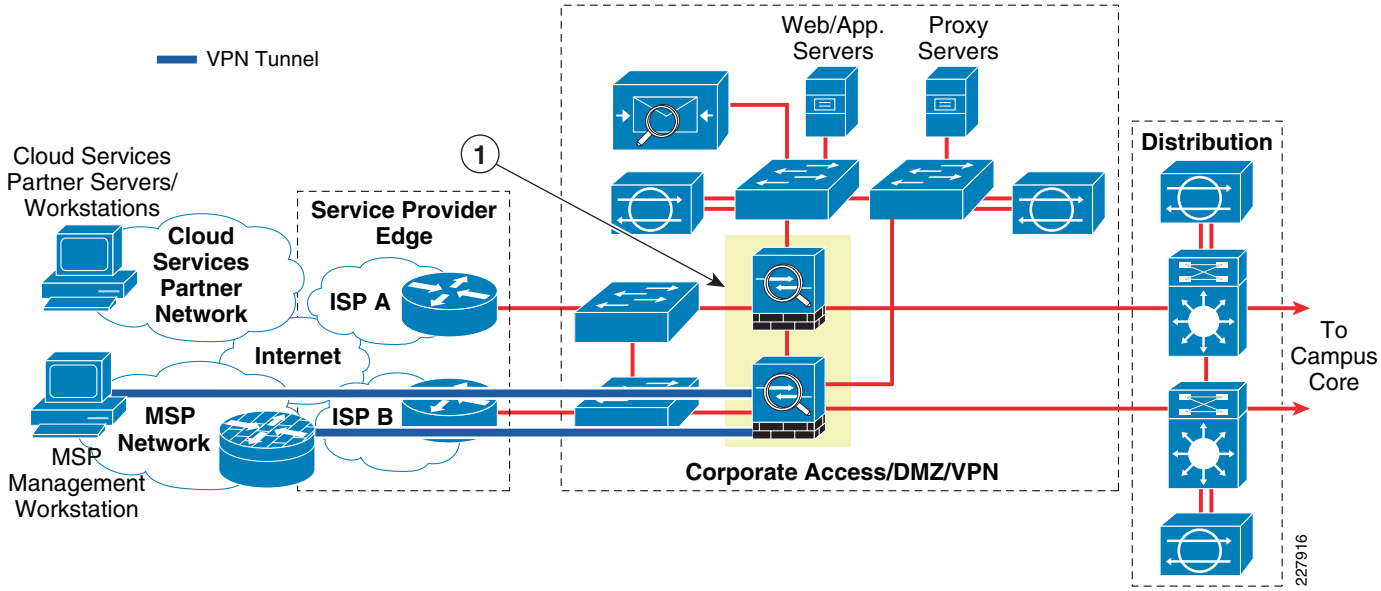
In Example 4-5, the default route to the Internet for the Building Infrastructure Network (BIN) VRF is pointed toward the Extranet DMZ firewall, instead of the Internet Edge firewall. Virtual firewall contexts are also not required within the Extranet DMZ firewalls to support this configuration. Instead a separate

physical interface on the Extranet DMZ firewalls can be provisioned, dedicated for the energy management solution VRF, as long as there is no overlapping IP address spaces between the global VRF and the energy management solution VRF.

Collapsed Internet Edge Designs

Although large organizations often deploy separate Internet Edge and Partner Extranet Modules with separate components for each function (firewall, remote access VPN, site-to-site VPN, etc.), smaller organizations sometimes collapse partner connectivity and employee Internet connectivity into a single module. The benefit of this design is reduced capital expenditures for networking equipment. However the disadvantage of this design is that there is no longer a clean separation of the MSP partner traffic from employee traffic into and out of the enterprise network. Also combining multiple functions into a single device increases the operational complexity of the device and reduces the overall scalability of the solution. However, for smaller organizations the trade-off is often acceptable. Figure 4-13 shows an example of a collapsed Internet edge design, as it applies to the energy management solution.

Figure 4-13 Example of a Collapsed Internet Edge Design



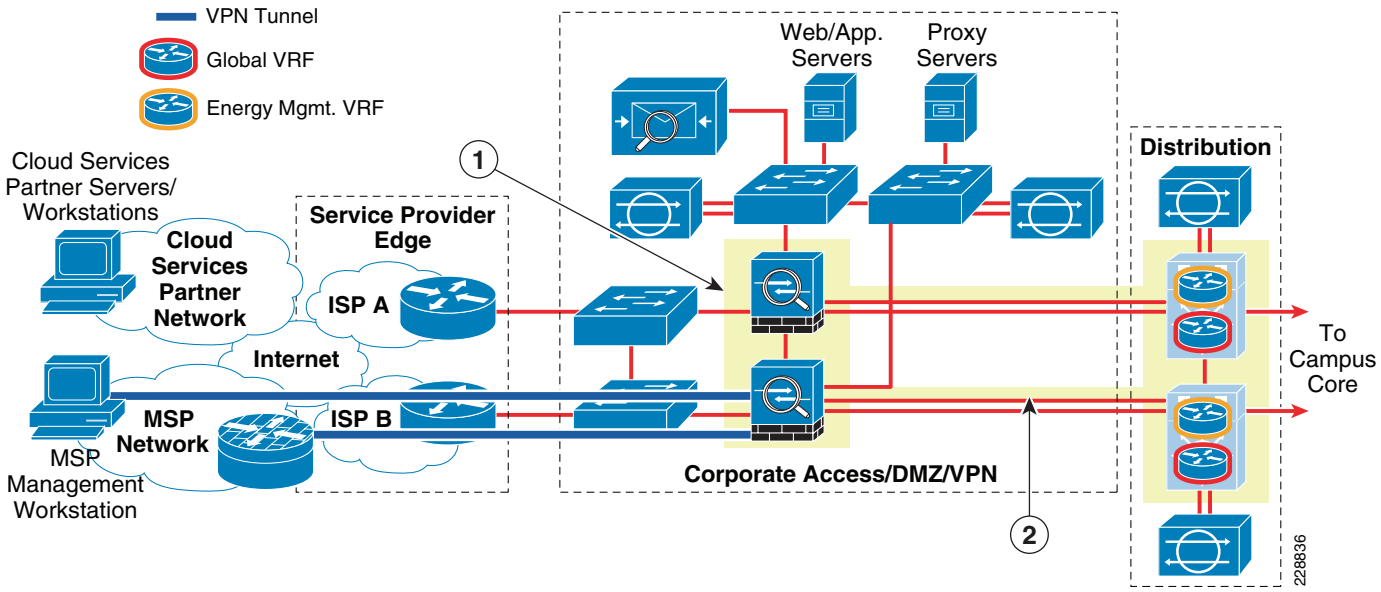
The following describes the number in Figure 4-13.

- **1**—ASA 5500 Security Appliances deployed within the corporate access/DMZ/ VPN section provides address translation and stateful access control for outgoing connections to cloud services partners. ASA 5500 Security Appliances also provide site-to-site and/or remote access VPN termination, address translation, IP address assignment, and stateful access control to MSP partner VPN connections.

With this design, a single pair of ASA 5500 Series Security Appliances can provide both site-to-site and remote access VPN connectivity for MSP partner and employee access, as well as stateful firewalling for Internet connectivity. As with the separate Partner Extranet Module design, the periodic export of data logs from the Mediators can be sent directly to cloud-services partner servers accessible through the Internet or sent via either a proxy or drop-and-forward server located on the DMZ. A separate energy

management VRF can also be extended to the ASA 5500 Series Security Appliances via a separate physical interface in order to provide path isolation for traffic to and from the Cisco Network Building Mediators, as is shown in Figure 4-14.

Figure 4-14 Example of a Collapsed Internet Edge Design with VRF



The following describes the numbers in Figure 4-14:

- **1**—ASA 5500 Security Appliances deployed within the corporate access/DMZ/VPN section provides address translation and stateful access control for outgoing connections to cloud services partners. ASA 5500 Security Appliances also provide site-to-site and/or remote access VPN termination, address translation, IP address assignment, and stateful access control to MSP partner VPN connections.
- **2**—Energy management VRF extended from the Catalyst 6500 switch within the distribution section of the collapsed Internet edge to a separate interface on the ASA 5500 Security Appliance.