Virtualization, Isolation and Encryption of IP Video Surveillance

This document demonstrates how to secure and logically separate an enterprise network to support IP Video Surveillance. The design described in this document implements the concepts of virtualization, path isolation, and encryption at both branch and campus LAN/WAN. If remote users have a business requirement to view live and archived video feeds, an option to provide an authenticated and secure VPN connection is also shown.

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Definitions and Goals

The term *network virtualization* is the creation of logical isolated network partitions over a common network infrastructure. The concept of virtualization of computing resources is not new, IBM released the operating system Virtual Machine Facility/370 in 1972. This software implemented a virtual hardware architecture on IBM 370 hardware. The primary advantage of virtualization for network or computing resources is to share a common hardware within the bounds of isolating the address space of one user from another.

In networking terms, *path isolation* is an important component of virtualization and it describes the creation of independent logical traffic paths over a shared physical network infrastructure. Path isolation is implemented in LAN switches by means of virtual LANs (VLANs). In WAN environments, path isolation is typically implemented through the use of virtual circuits. Both Frame-Relay and ATM include the concept of virtual circuits. Physically separate circuits can be associated with a Virtual Routing and Forwarding Lite (VRF-Lite) instance, a virtual router, and isolated from other VRF instances or the global routing table. Generic Routing Encapsulation (GRE) or IPSec encrypted tunnels can also be configured to provide path isolation. Examples of this are shown in "Configuring DMVPN Tunnel Interface" section on page 13, a Cisco IPsec/GRE solution.

By implementing VLANs, VRF-Lite and optionally IPSec/GRE, the network manager can provide access to a common network infrastructure while maintaining a separate address space, broadcast domain, and separation of one user group from another. *Segmentation* is the term often used to describe this technique and is synonymous with the term *isolation*. In layman's terms, network virtualization is a general concept, while path isolation is specific to maintaining a separation of the isolated network partitions between two points in the topology.

Historically, the physical security manager and the network manager had little interaction between their respective responsibilities. The physical security manager relied on a network infrastructure of coaxial cable (COAX) between camera, matrix switch, CCTV monitor, and networked digital video recorder (NDVR). Twisted pair (RS-485) is deployed for Pan Tilt Zoom control of analog cameras. The key requirement of any video surveillance implementation is the three Rs: *resolution, retention, and reliability*. Resolution in analog deployments is typically '4CIF/30', meaning 704x576 pixels at 30 frames per second. Retention is based on the number of days and is either regulated by a government agency, such as the State of Nevada Gaming Control board, a corporate policy, or the necessities of costs and the available disk space. Reliability is accomplished through a combination of the separate physical cable plant and human controls verifying the usefulness of the video images.

In many cases the physical security manager is going to be more confident in his ability to address the surveillance needs of the enterprise with a reliable, physically separate, cable plant for which he has total control.

Historically neither the physical security manager of value added resellers (VARs) are experts in IP networking. Therefore, the idea of transporting video over the enterprise IP network, with cameras sharing the same network with end-user workstations, servers, voice over IP (VoIP), and Internet traffic is an unknown, a cause for concern for the physical security manager. The physical security manager now must rely on the network manager for some degree of success and this is a barrier to acceptance.

Techniques to Achieve Virtualization

There are two primary techniques used to achieve network virtualization: policy-based and control plane-based. In this section, both techniques are implemented in a synergistic fashion to logically separate the video surveillance traffic from the other network traffic.

Policy-Based

Policy-based network virtualization restricts the forwarding of traffic to a specific destination based on some rule or administrative policy. These policies are independent of the control plane, meaning the destination is reachable and it may be listed in the routing table, but it is administratively prohibited. The most common implementation example is an access control list (ACL) on a router or firewall.

To implement policy-based controls, the router or firewall examines IP packets entering an interface and either forwards or drops packets based on matching fields in the IP header, transport header, or in more advanced implementations, some character string or fields in the payload of the packet. Firewalls also implement general policy-based matches on the security level of the source and destination interface of the packets. By default, firewalls permit packets to flow from a higher (more trusted) interface to a lower (less trusted) interface and the return path of that session is dynamically permitted. Packets that must be permitted from the less to more trusted interface must be explicitly defined and permitted.

Control Plane-Based

Control plane-based network virtualization is implemented by restricting the propagation of routing information. In other words, the routing tables are virtualized. The IP networks are segregated by their respective virtual routing table, or VPN routing and forwarding (VRF) table. VRF-Lite is one method of segmenting the routing tables, by creating virtual routing domains. These domains may reuse the same IP network addresses, they need not be globally unique. The can use separate address spaces from the remainder of the enterprise network or private address spaces based on RFC 1918 addressing. However, to aid in troubleshooting, it may be easier for the enterprise network manager to allocate unique IP addressing to each VRF domain. Allocating address space that facilitates summarization is as applicable to a VRF as is the case with routes in the global routing table.

Both policy-based and control plane-based techniques can be implemented in a synergistic approach to segment the network. The topology implemented in this sample deployment demonstrates both techniques. A firewall is implemented to connect the global routing table and the IP video surveillance domain (IPVS VRF) to allow a controlled and restricted access between the two domains.

IPSec Encryption

IPSec encryption provides privacy of the data, voice, and video on an IP network. Digital signatures is an important component of any IPSec implementation, providing authenticity (verifying the identity of the peer) and hashing techniques provide integrity (verifying packets have not been manipulated in transit).

In many encryption implementations, a logical tunnel interface joins two or more crypto peers, which in itself facilitates path isolation. Dynamic Multipoint VPN (DMVPN), generic routing encapsulation (GRE) over IP Security (IPSec) , IPSec/GRE, and Static Virtual Tunnel Interfaces (SVTI) are all examples of logical tunnel implementations. Group Encrypted Transport VPN (GET VPN) and Secure Sockets Layer virtual private network (SSL/VPN) are examples of payload encryption that have no logical tunnel interface. An IPSec implementation based on logical tunnels is more applicable to path isolation than payload encryption, because the logical tunnel endpoints can be in the global routing table with the tunnel itself residing in a VRF.

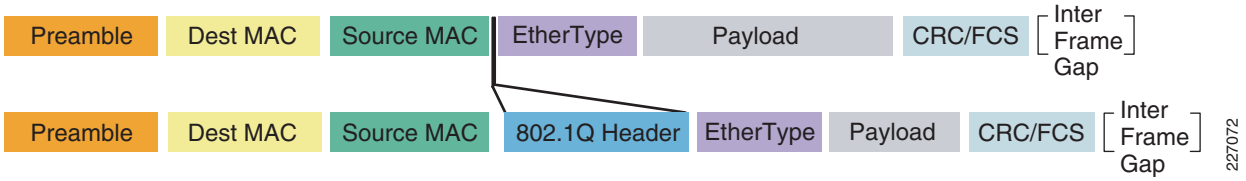
Multiple logical tunnels may be transported over a single physical path, providing an effective means of path isolation without the additional costs of a separate physical circuit. Alternately Layer-2 virtual circuit such as is implemented by ATM, 802.1Q trunking or Frame Relay could also be used, but there is no inherent privacy, authentication, or integrity component as with IPSec.

Path Isolation for LANs

In a campus LAN environment, IEEE 802.1Q (also known as VLAN tagging) is a means of associating a VLAN identifier with a Ethernet frame. This facility allows multiplexing several VLANs over the same physical switch and links between other switches, routers, and hosts. This allows for path isolation in a Layer-2 LAN in a campus or Metro-Ethernet service provider.

The Ethernet frame is not encapsulated, as is the case with IPSec or GRE tunnels; rather, a header is inserted between the source MAC address and the EtherType field in the frame. This concept is shown in Figure 1.

Figure 1 Ethernet Frame with VLAN Tagging



The 802.1Q header contains two fields of interest to the network manager: the VLAN identifier and the priority code point, or IEEE 802.1p class-of-service (CoS). The CoS field may be used to mark packets for the purpose of Layer-2 prioritization. The Cisco 4000 Series IP cameras can mark both CoS (Layer-2 QoS) and DSCP (Layer-3 QoS). Many LAN switches can prioritize frames based on the Layer-3 DSCP value so the use of Layer-2 QoS marking may be of less importance than the VLAN identifier associated with a tagged frame.

Note *CSCsz45893 Layer-2 CoS (802.1Q/p) for 4000 Series IP Camera* provides more information on the switch port configuration to support this feature.

In the topology demonstrated in this section, IP cameras are attached to switch ports that are configured as access ports associated with the appropriate VLAN, and the branch ISR routers are connected to the switch over an IEEE 802.1Q trunk link. This configuration allows both corporate end-users to share the same switch chassis as the IP video surveillance cameras, while maintaining isolation through unique VLANS and IP addressing.

Path Isolation for WANs

The ability to provide access from a central command center to video surveillance systems located at remote or branch offices is a key business driver for deploying IP-based systems. Many retail organizations currently create a physical CD-ROM / DVD of video feeds needed by the command center and use an overnight courier service to transport the media. Alternately, the investigation team may travel to the store location and view the video archive in-person at the store. Both of these methods of exchanging the video archive are costly and introduce delay of one or more days. Given the business requirement to demonstrate segmentation for IP video surveillance and the need to view video from a branch by the central command center, the WAN must therefore extend the segmentation between VLANs at the branch and command center.

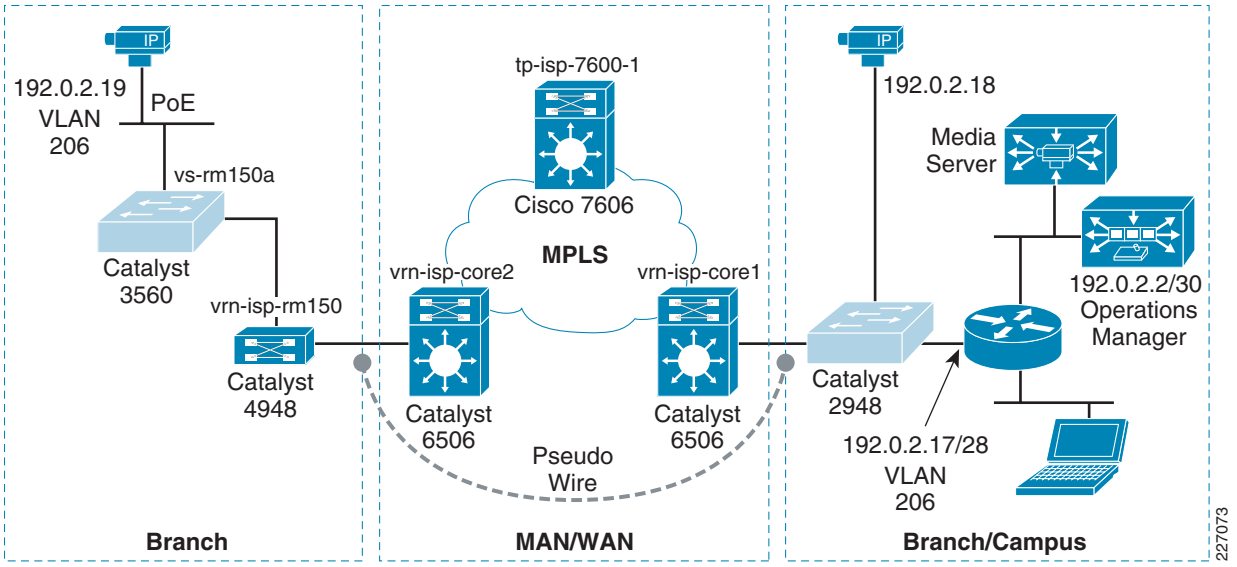
While segmentation with VLANs on a single switch incurs no costs, provisioning physically separate WAN circuits to connect these VLANs may be cost prohibitive. While Layer-2 virtual circuits based on Frame Relay and/or Frame Relay/ATM service interworking could be used to extend these LANs and provide path isolation, the exiting branch access circuit will likely have insufficient bandwidth. Many legacy branch access circuit data rates are typically at T1/E1 (1.5/2.0 Mbps) or less. As a rule of thumb, a standard definition IP camera requires approximately 1 Mbps and a high definition IP camera requires 3 to 4Mbps per feed.

Branches with access-circuits of dedicated leased lines (T1/E1 or DS3) that have no concept of a virtual circuit at the data link layer can be logically segmented by the use of multiple IPSec or GRE tunnels traversing the physical circuit. The test topology in this section demonstrates how to implement path isolation with IPSec tunnels (specifically DMVPN) as well as with Layer-2 path isolation using VLANs simulating a Metro-Ethernet type deployment.

As a best practice, video feeds from the cameras are stored to the local disk subsystem of the Media Server. The WAN connectivity between branch and campus location is segmented by VRF-Lite. Video is stored locally and only transported over the WAN occasionally for investigative purposes. As a point of reference, it is possible to implement a MPLS pseudowire deployment such that a camera at a remote location appears to be attached to the same LAN segment local to the Media Server and Operations Manager, and viewing stations.

This topology is illustrated in Figure 2.

Figure 2 MPLS Pseudowire Deployment



One practical application of this topology is a deployment where no corporate user-access is required and a single camera is sufficient for the business needs at the remote location. However, because the video feed is transmitted across the MPLS pseudowire WAN before being archived on the Media Server, packet loss must be managed by the service provider SLA and QoS marking, shaping, and queueing by both the enterprise and service provider. Costs in this deployment must also be considered, because the access circuit will likely be a dedicated T1/E1 that could be cost prohibitive. Single camera deployments may be better served by a teleworker class router, such as a Cisco 880 Series and a business class broadband access circuit.

While this topology may be implemented, the recommended solution is to store video locally, as close to the camera generating the feed as practical, and only transport across the WAN for occasional viewing or off-hours backup.

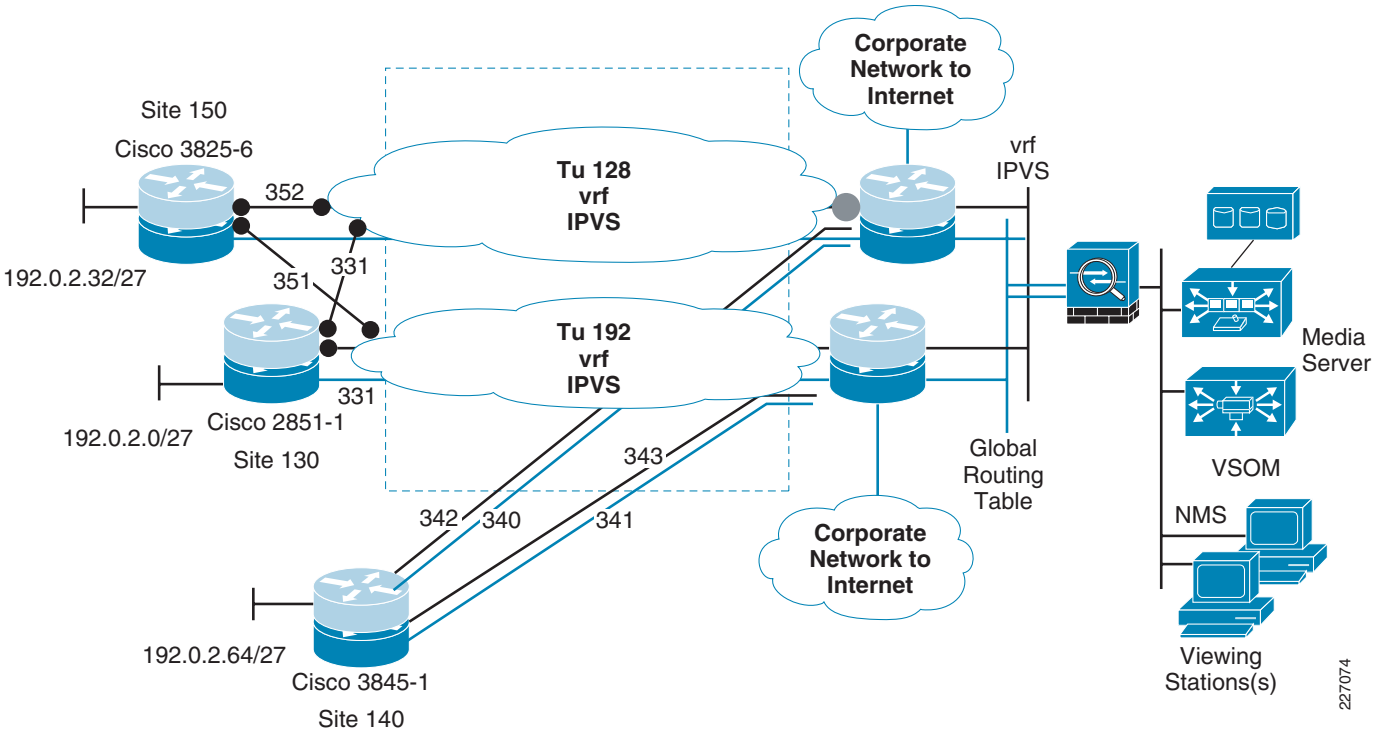
Implementing Virtualization

In this section the configuration of the switches, routers, and firewalls are discussed and the relevant configuration commands are shown to implement network virtualization and path isolation to segment the IP video surveillance devices and end-points from the global routing table. This segmentation of the network is accomplished by isolation of the control plane and network address space at the branch locations and campus command center by the use of VRF-Lite to create virtual routing tables. IP networks are comprised of both Layer-3 (routed) and Layer-2 (switched) domains. VRF-lite (VRFs without MPLS) is used in this enterprise network example to implement a virtual routing protocol instance. To provide end-to-end segmentation, both Layer-2 and Layer-3 are virtualized and mapped to each other accordingly.

Topology Diagram

The testing topology used is shown in Figure 3.

Figure 3 Virtualization Topology



In Figure 3, there are three branch locations each with a single Cisco ISR router. Both blue and grey router icons are shown to represent virtualization of the routing table. The blue icons represent the global routing table and the grey router icons represent the IPVS virtual routing table. The WAN aggregation routers shown in the center of the diagram terminate the branch locations and connect to the corporate network and Internet through separate DMVPN tunnels. These aggregation routers therefore are tunnel aggregation routers for the branches in the topology, and are spoke routers for connectivity to the corporate network. The aggregation routers are configured with HSRP on both the global routing table interface to the firewall as well as the IPVS interface.

Topology Description

In Figure 3, the Video Management and Storage System (VMSS) and Analog Video Gateway (AVG) network modules are logical interfaces. They, along with the DMVPN tunnel interfaces, are mapped to a Layer-3 domain: the VRF. The tunnel source and destination IP address are in the global routing table while the logical tunnel interface itself is in the video surveillance VRF. This separate VRF is named IPVS (for IP Video Surveillance). The iSCSI appliances, IP cameras, and viewing stations reside on a VLAN separate from the underlying corporate IP network and is in the IPVS VRF.

There are three branches shown in this topology example. Two branches demonstrate the deployment of DMVPN and one branch uses multiple virtual circuits (simulating MetroE MAN/WAN) for path isolation. At the branch locations, the iSCSI servers and IP cameras are in their own unique VLANs, which are dedicated to their respective function. Separate VLANS exist for the normal end-user traffic at the branch location and access to these devices are accomplished through the existing global routing table.

To demonstrate policy-based access control, a Cisco ASA5510 firewall is deployed at the command center location. This firewall includes two external interfaces, one in the global routing table and a second in the IPVS VRF. The inside, or most secure interface, is connected to a LAN switch and a VLAN to support the command center Media Server, VSOM, cameras, storage servers and viewing stations are deployed. This inside interface uses a subnet of the IP network address space allocated to the IPVS VRF. Access to the command center VLAN is controlled by firewall policy and static IP routes on the core routers and firewall. The NAT/pNAT configuration on firewall as well as the security levels and access-list permits communication from the IPVS VRF to the global routing table, provided that the session is initiated from the command center VLAN. There is no inbound global routing table access permitted to the IPVS VRF; only the return path to established sessions are permitted. Next, controlled inbound access is implemented by deploying a VPN concentrator.

The VPN concentrator (Cisco VPN 3000 Series) is added to the topology to allow access for selected users in the global routing table to the command center VLAN. The Cisco VPN client on the workstations connects to the VPN concentrator to authenticate the end-user and create a private and secured access to view live or archived video feeds. Adding the concentrator demonstrates a technique by which an external agency, such as a law enforcement department, can be provided with secured and authenticated access over the Internet/extranet.

Because the VPN concentrator allocates an IP address from the IPVS VRF address space, no NAT/pNAT exists inside the crypto tunnel. There are issues with access to a VSOM/Media Server web addresses and ports when these devices are behind a NAT/pNAT device. This is discussed in a separate section.

Address Table

Details of the IP addressing scheme in use for the following topology examples is shown in Table 1.

Table 1 Virtualization IP Addressing Scheme

Routing Table/VLAN	IP Address	Comments
WAN/MAN Global	192.168.15.0/26	MAN/WAN Interfaces (w/ crypto)
vpn4-3800-6 351	192.168.15.28/30	GigabitEthernet0/0.351
vpn4-3800-6 351	192.168.15.28/30	GigabitEthernet0/0.351
vpn4-3800-6 352	192.168.15.48/30	GigabitEthernet0/0.352
Global	10.81.7.0/24	Enterprise end-user
vpn4-3800-6 203	10.81.7.88/29	GigabitEthernet0/0.203

Table 1 Virtualization IP Addressing Scheme (continued)

Routing Table/VLAN	IP Address	Comments
WAN IPVS vrf	192.168.15.64 /26	MAN/WAN Interfaces (w/o crypto)
DMVPN Tu128 IPVS vrf	192.168.15.128/26	vpn-jk2-7206-1 Headend
DMVPN TU192 IPVS vrf	192.168.15.192/26	vpn-jk2-7206-2 Headend
IP VS Net IPVS vrf	192.0.2.0/24	Branch / Command Center Cameras, VSOM, AVG, Media Svr
vpn4-3800-6 IPVS vrf	192.0.2.32/27	Null0 - summary
vpn4-3800-6 IPVS vrf	192.0.2.32/30	Integrated-Service-Engine2/0 (VMSS)
vpn4-3800-6 IPVS vrf	192.0.2.36/30	Video-Service-Engine1/0 (AVG)
vpn4-3800-6 208	192.0.2.48/28	GigabitEthernet0/0.208 (Cameras)
iSCSI IPVS vrf	192.168.nnn.0/24	iSCSI Mgmt networks
vpn1-3845-1 256	192.168.11.0/24	
vpn1-2851-1 254	192.168.111.0/24	
vpn4-3800-6 258	192.168.211.0/24	

Implementation Overview

In the following sections, sample configuration files are shown to demonstrate the techniques used in creating a virtualized network for IP Video Surveillance. These steps include:

- Defining the VRF and Mapping Logical Interfaces
- Mapping Layer-2 (VLAN) to Layer-3 (VRF)
- Configuring VRF-Aware Routing Protocol
- Configuring DMVPN Tunnel Interface
- Configuring WAN Aggregation Router
- Configuring Firewall Interface
- Configuring Firewall Management Interface and Software Version
- Configuring Firewall Routes, Access-lists and NAT/pNAT
- Configuring Policy-based Features of Cisco IP Surveillance Cameras

Defining the VRF and Mapping Logical Interfaces

On the branch router, the VRF is defined and the logical interfaces of the AVG and the VMSS network module are associated with the VRF by the **ip vrf forwarding** interface command. The following is an example from one branch router, vpn4-3800-6:

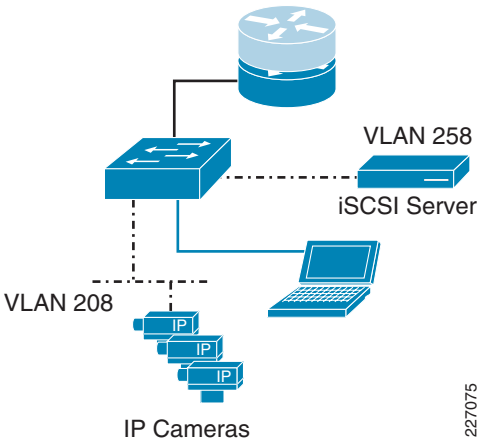
```
hostname vpn4-3800-6
!
ip vrf IPVS
 rd 100:10
 route-target export 100:10
 route-target import 100:10
!
```

```
!
interface Video-Service-Engine1/0
 description EVM-IPVS-16A
 ip vrf forwarding IPVS
 ip address 192.0.2.37 255.255.255.252
 ip route-cache flow
 service-module ip address 192.0.2.38 255.255.255.252
 service-module ip default-gateway 192.0.2.37
 no keepalive
!
interface Integrated-Service-Engine2/0
 description NME-VMSS-HP16
 ip vrf forwarding IPVS
 ip address 192.0.2.33 255.255.255.252
 ip route-cache flow
 service-module external ip address 192.168.211.2 255.255.255.0
 service-module ip address 192.0.2.34 255.255.255.252
 service-module ip default-gateway 192.0.2.33
 no keepalive
!
```

Mapping Layer-2 (VLAN) to Layer-3 (VRF)

IP networks are comprised of both Layer-2 (switches) and Layer-3 (routers) devices. To provide for end-to-end segmentation, the VLANs and the VRF must be mapped together. An association between Layer-2 and Layer-3 must be established. Using the branch topology as an example, the IP cameras are attached to access ports in VLAN 208 with an IEEE 802.1Q trunk port connecting the switch and the ISR router. The IPVS iSCSI server is on VLAN 258. The end-user workstations are in the global routing table. The topology is shown in Figure 4.

Figure 4 Mapping VLAN to VRF



The following sample configuration shows the router sub-interface for VLAN 208 and 258. They are associated with the IPVS VRF.

```
vpn4-3800-6#
!
interface GigabitEthernet0/0.208
 description inside interface for ip cameras
 encapsulation dot1Q 208
 ip vrf forwarding IPVS
 ip address 192.0.2.49 255.255.255.240
```

```
!
interface GigabitEthernet0/0.258
 description iSCSI Management Subnet
 encapsulation dot1Q 258
 ip vrf forwarding IPVS
 ip address 192.168.211.1 255.255.255.0
!
```

From the switch configuration, the uplink port to the ISR router and the access port for the IP camera is shown. The port for the iSCSI server would be similarly configured as the camera, but in VLAN 258. The following is a sample configuration:

```
!
interface GigabitEthernet1/0/1
 description trunk to vpn4-3800-6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 load-interval 60
 priority-queue out
 mls qos trust dscp
!
interface GigabitEthernet1/0/2
 description CIVS-IPC-2500
 switchport access vlan 208
 switchport mode access
end
```

The mapping of the VLAN to VRF is the responsibility of the supporting router, as the VLAN ID and the VRF name are associated with each other, because both references share the router sub-interface configuration.

Configuring VRF-Aware Routing Protocol

The branch router has interfaces in both the global routing table as well as the IPVS VRF and both network address spaces must be defined to the routing protocol. In the following example, EIGRP is the routing protocol used to illustrate the configuration.

```
!
router eigrp 65
 network 10.81.7.88 0.0.0.7
 network 192.168.15.0 0.0.0.63
 no auto-summary
 !
 address-family ipv4 vrf IPVS
  network 192.0.2.32 0.0.0.31
  network 192.168.15.128 0.0.0.127
  network 192.168.211.0
  no auto-summary
  autonomous-system 65
 exit-address-family
!
```

In the above sample configuration:

- Subnet 192.0.2.32/27 is for the AVG and VMSS network modules and IP cameras.
- Network 192.168.15.128/25 is for the DMVPN tunnels.
- Network 192.168.211.0/24 is for the iSCSI server at this branch.

- In the global routing table, 10.81.7.88/29 is for the end-user workstations and network 192.168.15.0/26 is for the WAN interfaces connecting this branch to the hub routers.

To display an instance of the virtual routing table associated with IPVS, the target VRF must be specified as shown in the following example:

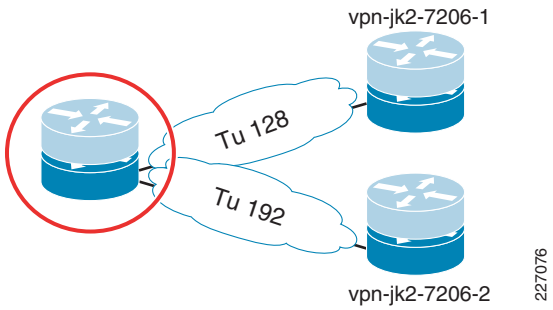
```
vpn4-3800-6#show ip eigrp vrf IPVS neighbors
IP-EIGRP neighbors for process 65
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.15.129          Tu128             14 01:17:47  134  5000  0  182
0   192.168.15.193          Tu192             10 01:17:47  132  5000  0  167
```

In the following section, the DMVPN tunnel interface configuration is shown for Tunnel 128. Tunnel 192 is configured similarly but not shown.

Configuring DMVPN Tunnel Interface

In this section, the configuration from one of the two tunnels of the branch router is shown (see Figure 5). The crypto topology deployed is a DMVPN dual-hub, dual-cloud implementation.

Figure 5 DMVPN Tunnel Interface Configuration



This branch router has a point-to-point Metro-Ethernet MAN link to the primary headend router, vpn-jk2-7206-1. This interface is in the global routing table and is VLAN 332 through the service provider network.

```
!
interface GigabitEthernet0/1.332
 encapsulation dot1Q 332
 ip address 192.168.15.46 255.255.255.252
!
```

The logical tunnel interface is in the IPVS VRF, the tunnel source is the above interface in the global routing table and the destination is Loopback 0 interface on vpn-jk2-7206-1, which is also in the global routing table.

```
!
interface Tunnel128
 ip vrf forwarding IPVS
 ip address 192.168.15.130 255.255.255.192
 ip mtu 1400
 ip nhrp authentication FOO
 ip nhrp map 192.168.15.129 192.168.15.40
 ip nhrp map multicast 192.168.15.40
 ip nhrp network-id 128
 ip nhrp nhs 192.168.15.129
 ip summary-address eigrp 65 192.0.2.0 255.255.255.224 5
 tunnel source GigabitEthernet0/1.332
```

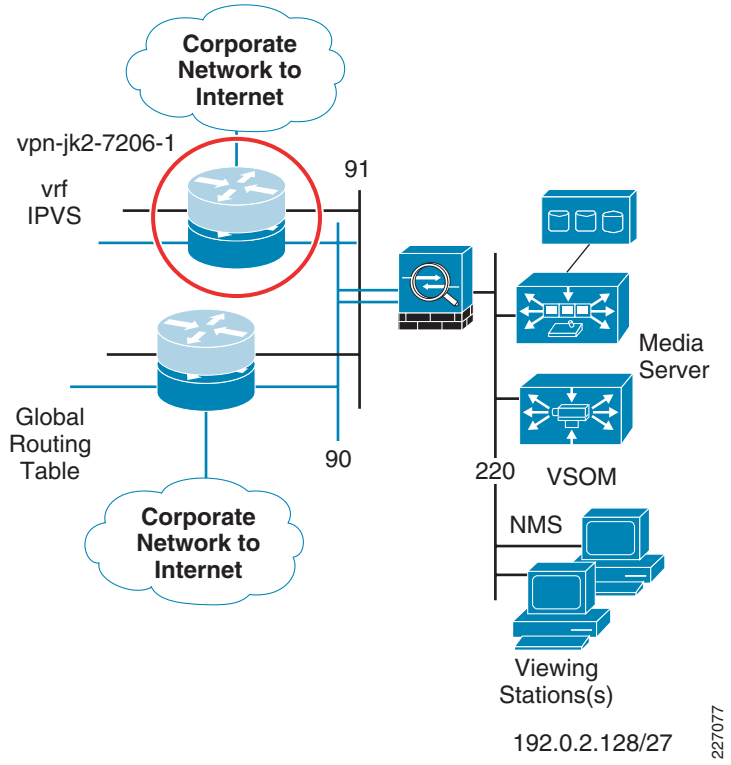
```
 tunnel destination 192.168.15.40
 tunnel key 128
 tunnel protection ipsec profile IPVS_Branches_ipsec_profile
!
ip route 192.168.15.40 255.255.255.255 192.168.15.45 name vpn-jk2-7206-1_Loopback_0
!
end
```

A static route to the tunnel destination is included so that this tunnel interface has an affinity to the physical interface; Tunnel 128 traffic is always transported over VLAN 332.

Configuring WAN Aggregation Router

This section examines the interfaces and topology of the WAN aggregation routers (see Figure 6). There are two WAN aggregation routers for high availability to the branch locations. Only one of these two similarly configured WAN aggregation router configuration is shown for the sake of brevity.

Figure 6 WAN Aggregation Router Configuration



The WAN aggregation router vpn-jk2-7206-1 has interfaces in both the global routing table and in the IPVS VRF. For clarity, the interfaces in the global routing table are shown in blue in the following sample configuration. The IPVS interfaces are shown in black text. The tunnel's logical interface is in the IPVS VRF while the tunnel source/destination IP addresses are in the global routing table.

```
vpn-jk2-7206-1#sh run b | beg interface Loopback0
interface Loopback0
 description Loopback for Global RT
 ip address 192.168.15.40 255.255.255.255
!
interface Tunnel128
 description DMVPN tunnel/cloud to Branches
```

```
 ip vrf forwarding IPVS
 ip address 192.168.15.129 255.255.255.192
 no ip redirects
 ip mtu 1400
 ip nhrp authentication FOO
 ip nhrp map multicast dynamic
 ip nhrp map multicast 192.168.15.40
 ip nhrp network-id 128
 ip nhrp nhs 192.168.15.129
 ip nhrp server-only
 ip route-cache flow
 no ip split-horizon eigrp 65
 ip summary-address eigrp 65 192.0.2.0 255.255.255.0 5
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 128
 tunnel protection ipsec profile IPVS_Branches_ipsec_profile
!
interface Tunnel300
 description DMVPN Tunnel to Enterprise/Internet
 ip address 10.81.7.254 255.255.255.240
 ip mtu 1400
 ip pim sparse-mode
 ip nhrp authentication BAR
 ip nhrp map multicast dynamic
 ip nhrp map 10.81.7.241 64.102.223.24
 ip nhrp map multicast 64.102.223.24
 ip nhrp network-id 22341
 ip nhrp nhs 10.81.7.241
 ip route-cache flow
 load-interval 30
 tunnel source FastEthernet0/0
 tunnel destination 64.102.223.24
 tunnel key 300
 tunnel protection ipsec profile DMVPN_IPSEC_PROFILE
!
interface FastEthernet0/1.90
 description ASA DMZ Global
 encapsulation dot1Q 90
 ip address 10.81.7.161 255.255.255.248
 ip flow ingress
 standby 0 ip 10.81.7.166
 standby 0 preempt delay minimum 60
!
interface FastEthernet0/1.91
 description ASA DMZ vrf IPVS
 encapsulation dot1Q 91
 ip vrf forwarding IPVS
 ip address 192.168.15.97 255.255.255.248
 ip flow ingress
 standby 0 ip 192.168.15.102
 standby 0 preempt delay minimum 60
!
!
interface FastEthernet0/1.332
 description MAN/WAN to Site 130 (vpn1-2851-1)
 encapsulation dot1Q 332
 ip address 192.168.15.45 255.255.255.252
 ip flow ingress
!
interface FastEthernet0/1.340
 description MAN/WAN to Site 140 (vpn1-3845-1)
 encapsulation dot1Q 340
 ip address 192.168.15.13 255.255.255.252
```

```
 ip flow ingress
!
interface FastEthernet0/1.342
 description MAN/WAN to Site 140 (vpn1-3845-1)
 encapsulation dot1Q 342
 ip vrf forwarding IPVS
 ip address 192.168.15.77 255.255.255.252
 ip flow ingress
 ip summary-address eigrp 65 192.0.2.0 255.255.255.0 5
!
interface FastEthernet0/1.352
 description MAN/WAN to Site 150 (vpn4-3800-6)
 encapsulation dot1Q 352
 ip address 192.168.15.49 255.255.255.252
 ip flow ingress
!
end
```

The Cisco ASA 5510 firewall is connected to the two WAN aggregation routers and there are FastEthernet interfaces in both the global and IPVS VRF to the firewall. Two of the three branch routers in this topology are cryptography-enabled and have a single MAN link between the branch and each aggregation router. One branch, vpn1-3845-1 (Site 140), router demonstrates a branch without crypto on the MAN, and to implement path isolation, there are two physical links, one in the global routing table and one in the IPVS VRF.

Connectivity from this central command center location to the remainder of the corporate network and to the Internet is provided by way of Tunnel300 in the global routing table.

Configuring Firewall Interface

Referring to the topology in Figure 6 on page 14, the firewall interface configuration is shown below. The blue text highlights the interface description in the global routing table while the interfaces in black text are associated with the VRF IPVS.

```
!
interface Ethernet0/0
 description Campus_IPVS VLAN 220
 nameif Campus_IPVS
 security-level 70
 ip address 192.0.2.129 255.255.255.224
!
interface Ethernet0/1
 description DMZ_IPVS VLAN 91
 nameif DMZ_IPVS
 security-level 50
 ip address 192.168.15.99 255.255.255.248
!
interface Ethernet0/2
 description DMZ_Global VLAN 90
 nameif DMZ_Global
 security-level 10
 ip address 10.81.7.163 255.255.255.248
!
```

In this topology, the firewall is functioning as a policy-based network virtual device and there are no interface configuration commands that make the ASA 5510 VRF-aware. The interface named *Campus_IPVS* is attached to VLAN 220 on the campus switch. Access to this address space from the global routing table and branch locations in the IPVS VRF is policy-based. The firewall configuration controls the access between the three interfaces.

Configuring Firewall Management Interface and Software Version

A management interface is connected to the lab FlashNet network to facilitate software upgrades and out-of-band (OOB) management of the firewall. The management interface-related commands are shown below and will not be referenced in any subsequent sections of this document.

```
!
interface Management0/0
 description FlashNET
 speed 100
 duplex full
 nameif FlashNET
 security-level 0
 ip address 172.26.156.3 255.255.254.0
!
route FlashNET 172.26.0.0 255.255.254.0 172.26.156.1 1
!
access-group MANAGEMENT in interface FlashNET control-plane
access-list MANAGEMENT extended permit tcp 172.26.0.0 255.255.254.0 interface FlashNET

http server enable
http 172.26.156.0 255.255.254.0 FlashNET
snmp-server location ESE Lab
snmp-server contact foo.bar@cisco.com
snmp-server enable traps snmp authentication linkup linkdown coldstart
!
telnet 172.26.156.0 255.255.254.0 FlashNET
telnet timeout 60
!
ssh 172.26.156.0 255.255.254.0 FlashNET
ssh timeout 60
console timeout 0
```

The software version used in testing is: as follows

```
vpn-jk2-asa5510-1# sh ver

Cisco Adaptive Security Appliance Software Version 8.0(4)
Device Manager Version 6.1(5)51

Compiled on Thu 07-Aug-08 20:53 by builders
System image file is "disk0:/asa804-k8.bin"
```

Configuring Firewall Routes, Access-lists and NAT/pNAT

The global routing table has the lowest security-level (ignoring the security-level 0 management interface, FlashNet) and this configuration is intended to deny access to the IPVS VRF from the outside. No access-lists are configured to permit inbound access. The branch locations are in the IPVS VRF which is at security-level of 50, lower than the security level of the command center at 70. For initiating access from a lower value security level to a higher value requires the definition of access-list.

The access-lists are configured on the firewall to permit the branch routers, switches, cameras and the iSCSI servers to send traffic to the network management server(s) located in the command center.

The following sample configuration assumes that syslog, snmptraps, NetFlow export (UDP port 7777) and any viewing stations at the branch (TCP to port 80 or WWWW) are permitted from the branch IPVS VRF to the command center.

```
!
access-list IPVS-CC extended permit udp any 192.0.2.128 255.255.255.224 eq syslog
access-list IPVS-CC extended permit udp any host 192.0.2.139 eq snmptrap
access-list IPVS-CC extended permit udp any host 192.0.2.139 eq 7777
access-list IPVS-CC extended permit tcp 192.0.2.0 255.255.255.0 any eq www
access-group IPVS-CC in interface DMZ_IPVS
!
```

For troubleshooting purposes, ICMP is also permitted. This can be disabled if specified by the security policy of the enterprise network.

```
icmp unreachable rate-limit 1 burst-size 1
icmp permit any Campus_IPVS
icmp permit any DMZ_IPVS
icmp permit any DMZ_Global
!
```

The two next-hop IP addresses in the following route statements are HSRP addresses configured on the WAN aggregation routers: 10.81.7.166 and 192.168.15.102. A default route is configured for the global routing table and routes to the IP addresses present in the IPVS VRF are shown.

```
route DMZ_Global 0.0.0.0 0.0.0.0 10.81.7.166 1
route DMZ_IPVS 192.0.2.0 255.255.255.0 192.168.15.102 1
route DMZ_IPVS 192.168.11.0 255.255.255.0 192.168.15.102 1
route DMZ_IPVS 192.168.111.0 255.255.255.0 192.168.15.102 1
route DMZ_IPVS 192.168.211.0 255.255.255.0 192.168.15.102 1
!
```

Tip In this example, the IP subnets for the iSCSI management networks are not allocated from contiguous address space. Had that been done, these three routes could have been consolidated into a single route, as is the case with the 192.0.2.0 network. Address allocation that allows summarization is an aid to reducing the size and complexity of configurations.

Lastly, the NAT/pNAT configuration implements the policy that the command center address space is port address translated (PAT) to the global interface IP address. No address or port translation takes place between the IPVS VRF address space at the branch locations and the command center.

```
global (DMZ_Global) 1 interface
nat (Campus_IPVS) 1 192.0.2.128 255.255.255.224
static (Campus_IPVS,DMZ_IPVS) 192.0.2.128 192.0.2.128 netmask 255.255.255.224
```

Configuring Policy-based Features of Cisco IP Surveillance Cameras

The Cisco 2500 Series IP cameras have several policy-based features that protect the camera resource from unauthorized access. There are three steps in initiating a video feed between the camera and the media server.

1. First, the authentication step, is initiated via HTTPS and as such the payload of this session is encrypted. The control plane negotiation, RTSP, and the video feed, RTP, are not secured by any payload encryption. The topology described in this section demonstrates how IPSec encryption can be implemented on the WAN to provide encryption and the resulting privacy of video feeds that leave the campus for live or archive viewing, or for archive backup.
2. The camera software includes access control, through userid and password, which is configured on both the camera configuration and the corresponding VSOM definition of the camera. Because the Cisco camera software allows only a single concurrent login, a unique account (userid) for the media server, when the camera is defined through VSOM, is recommended. This allows an administrator to be logged on the camera while the media server is starting or stopping video feeds. This aids in troubleshooting. The log files can be viewed in real-time without disrupting the command and control function of the media server.
3. The Cisco 2500 Series IP camera software, as many other vendor camera software does, provides an access control-list to permit or deny what IP addresses are authorized to attempt to access the camera. While implementations differ, one advantage of the Cisco implementation is the ability to define a range of IP address and either permit or deny access from that range. The addressing scheme deployed in this test topology uses 192.0.2.0/24 for branch and command center IPVS VRFs. The WAN interfaces and the iSCSI network address is in the 192.168.0.0/16 address space. Given this addressing scheme, a workstation in the command center in the 192.0.2.128/27 address space or the branch VMSS network modules at 192.0.2.2/32, 192.0.2.34/32 and 192.0.2.65/32, can access their respective cameras when all cameras are configured to:

   permit ip 192.0.2.0 255.255.255.0

   deny ip any

The advantage of selecting an address scheme that can be consolidated in this manner provides a simple configuration on all IP cameras in the network, yet provides a reasonable level of access control that does not require frequent updates.

Tip Both 192.0.2.0/24 and 192.168.0.0/16 are RFC3330 special use IPv4 addresses. 192.0.2.0/24 is assigned as *TEST-NET* and used in documentation and example code. 192.168.0.0/16 is used in private networks and is documented in RFC1918. Neither address block should appear, or be routed, on the public Internet.

Summary

This section addressed the need for implementing a logically separate IP network infrastructure to support an IP based video surveillance deployment in an existing enterprise network. Both control plane virtualization as well as policy-based techniques are deployed. IPSec encryption is also implemented to leverage the inherent path isolation of a logical tunnel as well as to make private the video feeds as they traverse the MAN/WAN. Access to resources outside the IPVS VRF must be initiated from hosts on the command center in order for the firewall to permit inbound packets. Because the IP addressing in use is based on addresses that are not routed on the public Internet, the firewall implements NAT/pNAT of these sessions from the IPVS VRF to the Internet or other enterprise address space.

In this next section, the configuration is enhanced to permit workstations external to the IPVS address space to view video feeds.

External Access to IPVS VRF

The goal of this section is to demonstrate a method of providing access to video feeds for viewing stations (PCs) that are in the global routing table, extranet, or even the Internet.

Topology Description

To accomplish this, a VPN concentrator, a Cisco VPN 3080, is deployed on the remaining unused interface on the Cisco ASA 5510 firewall. Client PCs connect to the VPN concentrator by installing the VPN 3000 client software from *www.cisco.com*. Access to the VPN concentrator is authenticated on a group name and key, as well as a userid and password. In these examples, the group/key and userid/password are stored locally on the VPN concentrator and can be administered by the command center security operations manager, or based on enterprise security policies, can be in an external database. The external authentication server database option improves scalability and manageability.

Because the VPN concentrator uses IPSec encryption, the video feeds that are leaving IPVS VRF through the command center VLAN are encrypted and hashed. In testing 3DES/HMAC-MD5 is used. To limit outside access to the VPN concentrator, the firewall is configured to permit inbound access to the outside interface of the VPN concentrator to only.

- UPD 500 (IKE)
- UDP 4500 (IKE/IPSEC with NAT-T)
- Protocol ESP (Protocol ‘50’)
- ICMP (for troubleshooting and verification of connectivity)

This firewall configuration, therefore, rejects all other packets that are not required for transporting the IKE/IPSec tunnels and ICMP (ping). This, in addition to deploying a group/key and userid/password to authenticate the end-users, is a commonly deployed best practice.

Alternatives to the VPN Concentrator

Cisco announced the end-of-sale and end-of-life dates for the Cisco® VPN 3000 Series Concentrators. The product becomes obsolete August 4, 2012. See the *EOL/EOS for the VPN 3000 Series Concentrators* document on www.cisco.com.

An alternative to the VPN concentrator is a remote access solution based on Secure Sockets Layer Virtual Private Network (SSL VPN). SSL VPN clients can be terminated on a Cisco ASA 5500 Series device or on a Cisco modular ISR routers (1800, 2800, 3800) with the appropriate SSL VPN hardware acceleration.

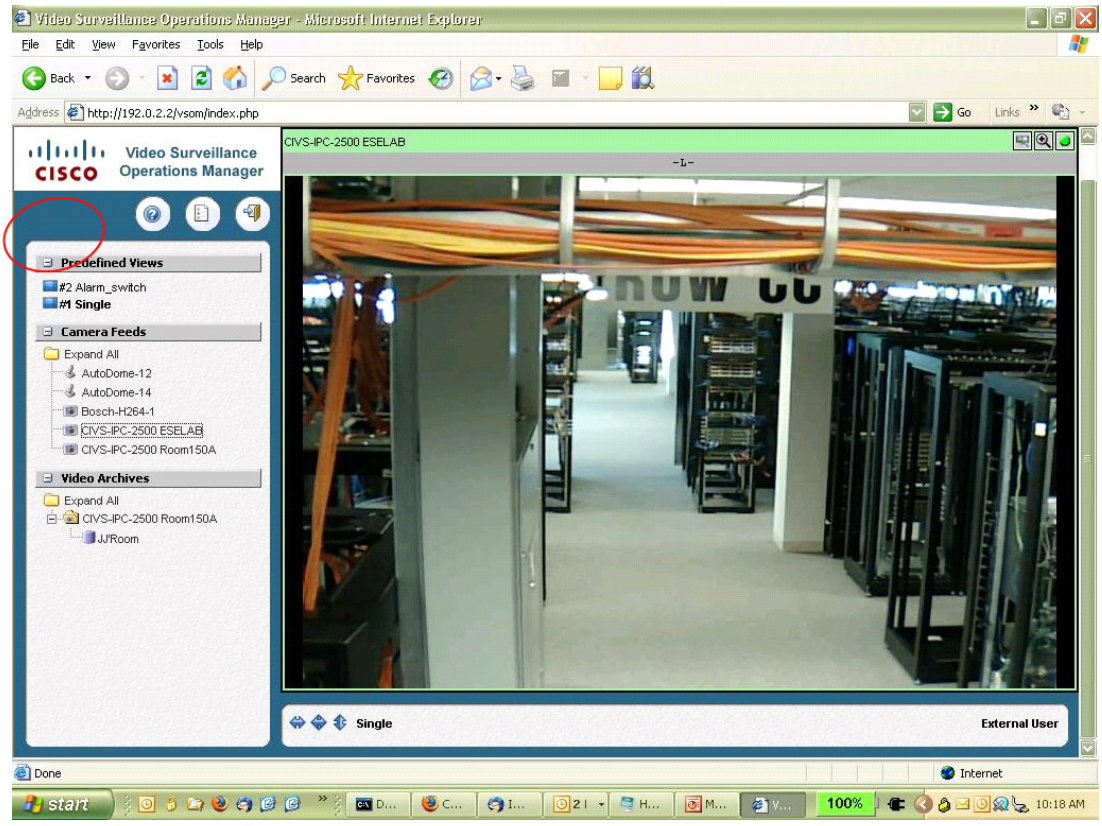
As a best practice, terminate the VPN concentration function on a device separate from the firewall. In other words, an ISR router or ASA device could be substituted for the VPN 3000 Series concentrator shown.

Limiting Authority in VSOM

Once the remote PC has connected and authenticated to the VPN Concentrator, the user has access to devices in the IPVS VRF. In the previous section, the policy-based features of the IP surveillance cameras are implemented to limit access to a configured address space within the IPVS VRF. The VPN concentrator is configured with an address pool that is not included in the IP camera access-list, which means users connecting through the VPN concentrator are not permitted direct access to the web server on the camera.

For remote users to view the live or archive video feeds, they must connect to the appropriate Video Surveillance Operations Manager (VSOM)/Media Server Web Server using a supported browser. To gain access to the video feeds, a userid and password must be entered. It is recommended that users are provided only the privileges necessary for their job function. In this case, the remote user only requires ‘operator’ privileges, and as such a user account is configured accordingly. When a user with only ‘operator’ privileges is logged on VSOM, no admin icon exists on the screen; the user may view live or archived video, but no configuration changes are permitted. A sample operator screen is shown in Figure 7.

Figure 7 Sample VSOM Operator Screen



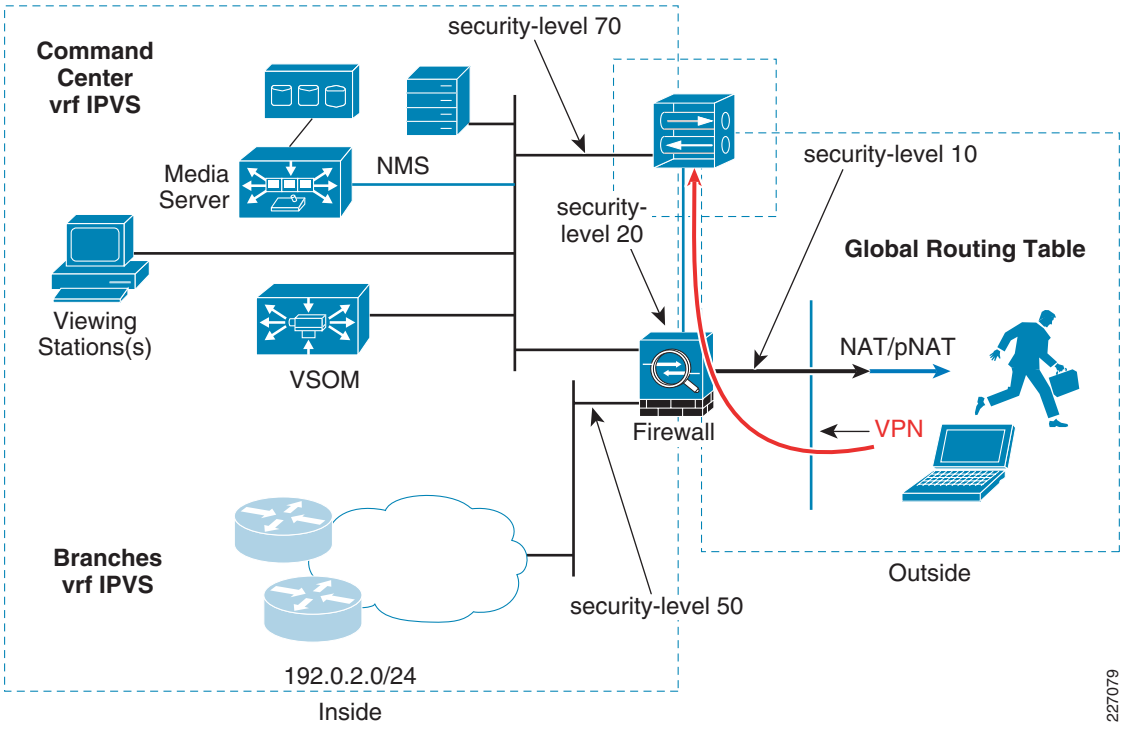
Other than the obvious differences associated with available bandwidth to the remote user, there is no difference in the presentation of the video feed for a remote user connected through the VPN concentrator versus a PC attached to the LAN in the command center.

Topology Diagram

The VPN concentrator consists of a public and private interface configuration. The public, or outside, interface is attached to the remaining unused interface on the ASA5510. The private (or inside) interface is attached to the LAN switch on VLAN 220, the command center VLAN. The security level of the ASA interface connecting to the VPN concentrator is 20. Because this value is numerically higher than the firewall outside interface with security-level 10, access-control lists are created on the firewall to allow the port numbers and protocols permitted to reach the VPN concentrator.

Figure 8 illustrates where in the topology the VPN concentrator is located.

Figure 8 Virtualization Topology with VPN Concentrator



The revised interface configuration of the ASA 5510 and the IP addressing for the VPN concentrator is shown in the following subsections.

Implementation Overview

To show how the VPN concentrator is deployed in the topology, the following configuration steps are implemented or updated from the previous sections.

- Configuring VPN Concentrator Interface and Address
- Configuring Firewall Interface
- Configuring WAN Aggregation Routing
- Configuring Firewall NAT/pNAT and Routing
- Configuring Firewall Access-lists
- Configuring VPN Concentrator User/Group/Proposals

Configuring VPN Concentrator Interface and Address

The public VPN concentrator interface is on a point-to-point network to the firewall. The VPN concentrator is at 10.81.7.57 and the firewall is at 10.81.7.58. The public interface in the global routing table is highlighted in blue. The management interface on FlashNET is shown, but is optional.

```
vpn2-3080-1: Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
--------------------------------------------------------------------------------
Ether1-Pri|      UP      |    192.0.2.136/255.255.255.224| 00.03.A0.88.3F.58
Ether2-Pub|      UP      |     10.81.7.57/255.255.255.252| 00.03.A0.88.3F.59
Ether3-Ext|      UP      |  172.26.157.15/255.255.254.0  | 00.03.A0.88.3F.5A
```

The remote clients are allocated an IP address from the configured pool. This assigned address is used to identify the remote PC inside the IPSec tunnel interface. The address pool list used in this configuration is five IP addresses from the 192.168.15.64/29 subnet. If more concurrent remote sessions are required, a larger IP address pool must be allocated. Allocate as a large a pool as required, but not more than necessary.

```
vpn2-3080-1: Address -> 2

  This is the Address Pool List

   Start Addr          End Addr          Subnet Mask
-------------------------------------------------------
 192.168. 15. 65 | 192.168. 15. 70 | 255.255.255.248 |
-------------------------------------------------------
```

The IP routing configuration on the VPN concentrator is straight forward. A default route is configured to the firewall IP address and a network route is configured to 192.0.2.0/24. As discussed in the previous sections, note the iSCSI devices and the WAN interfaces in the IPVS VRF are allocated from the 192.168.0.0/16 address space; therefore, with this configuration, the remote users can only reach IP hosts on the 192.0.2.0/24 subnet: the VSOM and Media Servers. The IP cameras are on the 192.0.2.0/24 subnet, but access-control lists prevent any connectivity from source IP address in the address pool 192.168.15.64/29.

```
vpn2-3080-1: Routing -> 1

Static Routes
-------------
Destination     Mask            Metric Destination
------------------------------------------------------------
0.0.0.0         0.0.0.0              8 10.81.7.58
172.26.0.0      255.255.0.0          1 172.26.156.1
192.0.2.0       255.255.255.0        8 192.0.2.129
```

Note The 172.26.0.0 network is lab FlashNet for management of the device.

Configuring Firewall Interface

The previously unused interface Ethernet 0/3 is now deployed as the point-to-point interface to the VPN concentrator. All other interfaces are the same as discussed in the previous sections. The interfaces in the global routing table are highlighted in blue.

```
vpn-jk2-asa5510-1# show run
: Saved
:
ASA Version 8.0(4)
!
hostname vpn-jk2-asa5510-1
domain-name ese.cisco.com
enable password [removed] encrypted
passwd [removed] encrypted
names
dns-guard
!
interface Ethernet0/0
 description Campus_IPVS VLAN 220
 nameif Campus_IPVS
 security-level 70
 ip address 192.0.2.129 255.255.255.224
!
interface Ethernet0/1
 description DMZ_IPVS VLAN 91
 nameif DMZ_IPVS
 security-level 50
 ip address 192.168.15.99 255.255.255.248
!
interface Ethernet0/2
 description DMZ_Global VLAN 90
 nameif DMZ_Global
 security-level 10
 ip address 10.81.7.163 255.255.255.248
!
interface Ethernet0/3
 description DMZ for VPN3080
 nameif DMZ_VPN3080
 security-level 20
 ip address 10.81.7.58 255.255.255.252
!
```

There is no NAT/pNAT address translation between Ethernet 0/2 and Ethernet 0/3. The WAN aggregation routers must have a route to the VPN concentrator IP address, 10.81.7.57.

Configuring WAN Aggregation Routing

The WAN aggregation routers needs to be configured to include the two additional IP networks which are required to support the VPN concentrator. These networks are the public interface and the IP address pool for the remote client workstations. In this sample topology, these networks are

- 10.81.7.56/30 —Public subnet
- 192.168.15.64/29—IP address pool

Because the WAN routers are not exchanging routing updates from the firewall and VPN concentrator, a static route for the public subnet must be added to the global routing table and redistributed to the dynamic routing protocol to update the global routing tables.

```
ip route 10.81.7.56 255.255.255.252 10.81.7.163 name ASA5510
```

The second route is included in the IPVS VRF, and is also redistributed to the dynamic routing protocol to inform the branch routers of this route.

```
ip route vrf IPVS 192.168.15.64 255.255.255.248 192.168.15.99 name VPN3080_pool
!
```

The remainder of the WAN aggregation routers configuration addresses defining these two networks in the appropriate prefix-list and route-map and then redistributing these networks under the appropriate autonomous system (AS) number and VRF.

```
ip prefix-list ASA5510_VPN3080 seq 5 permit 10.81.7.56/30
!
route-map ASA5510_VPN3080 permit 10
 match ip address prefix-list ASA5510_VPN3080
!
ip prefix-list COMMAND_CENTER seq 100 permit 192.0.2.128/25
ip prefix-list COMMAND_CENTER seq 101 permit 10.81.7.0/24
ip prefix-list COMMAND_CENTER seq 102 permit 192.168.15.64/29
!
route-map COMMAND_CENTER permit 10
 match ip address prefix-list COMMAND_CENTER
 set tag 2128
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map ASA5510_VPN3080
 redistribute eigrp 65 metric 1000 100 255 1 1500 route-map Branch_Networks
 passive-interface FastEthernet0/1.90
 network 10.0.0.0
 no auto-summary
 eigrp stub connected redistributed
!
router eigrp 65
 redistribute eigrp 64 metric 1000 100 255 1 1500 route-map DEFAULT
 network 192.168.15.0 0.0.0.63
 no auto-summary
 !
 address-family ipv4 vrf IPVS
  redistribute static metric 1000 10 255 1 1500 route-map COMMAND_CENTER
  network 192.168.15.64 0.0.0.63
  network 192.168.15.128 0.0.0.63
  distribute-list route-map Branch_Net_vrf_IPVS_RT in
  no auto-summary
  autonomous-system 65
 exit-address-family
!
```

Note EIGRP AS 64 is used to connect to the enterprise address space. EIGRP AS 65 is used to connect to the branch networks for both the global routing table and the IPVS VRF.

Configuring Firewall NAT/pNAT and Routing

The NAT/pNAT configuration on the firewall is changed by adding two static entries to the configuration deployed in the previous section. The first static entry for 192.168.15.56/30 defines that no address translation occurs between the outside global routing table and the point-to-point network address between the firewall and the concentrator.

The second static entry, for 192.168.15.64, defines that no address translation occurs for the IP address pool defined in the VPN concentrator for remote users and the IPVS VRF.

```
global (DMZ_Global) 1 interface
nat (Campus_IPVS) 1 192.0.2.128 255.255.255.224
!
static (DMZ_VPN3080,DMZ_Global) 192.168.15.56 192.168.15.56 netmask 255.255.255.252
static (Campus_IPVS,DMZ_IPVS) 192.0.2.128 192.0.2.128 netmask 255.255.255.224
static (Campus_IPVS,DMZ_IPVS) 192.168.15.64 192.168.15.64 netmask 255.255.255.248
!
```

A route in the firewall for the concentrator address pools is required. All other routes are the same as from the previous section.

```
route Campus_IPVS 192.168.15.64 255.255.255.248 192.0.2.136 1
!
```

Configuring Firewall Access-lists

In addition to the access-list and group IPVS-CC, documented in the previous section, with the addition of the VPN concentrator, access-lists permitting the protocols and ports needed for the encryption protocols are added to the firewall configuration. Protocol ESP, UDP 500 and 4500, and ICMP are permitted. This allows the remote VPN client to contact the concentrator.

```
access-group INBOUND in interface DMZ_Global
access-list INBOUND extended permit esp any host 10.81.7.57
access-list INBOUND extended permit udp any host 10.81.7.57 eq isakmp
access-list INBOUND extended permit udp any host 10.81.7.57 eq 4500
access-list INBOUND extended permit icmp any host 10.81.7.57

icmp permit any DMZ_VPN3080
!
```

The VPN concentrator is at IP address 10.81.7.57.

Configuring VPN Concentrator User/Group/Proposals

It is recommended to use an external database server for authentication in large deployments. A complete VPN concentrator configuration is outside the scope of this document, however, configuration notes for the miscellaneous configuration for the user, group, and IKE proposals are shown below.

```
vpn2-3080-1: User Management -> 2

                              Current User Groups
-------------------------------------------------------------------------------
| 1. foo (Internal)                    |                                      |
-------------------------------------------------------------------------------


vpn2-3080-1: User Management -> 3

Internal groups are configured on the VPN 3000 Concentrator's Internal Database.
ESP-3DES-MD5 with IKE Keepalive - Tunnel Type is Remote Access - Authentication Internal
IPSec UDP (allow NAT-T)

                                   Current Users
-------------------------------------------------------------------------------
| 1. aprilmay                          |                                      |
-------------------------------------------------------------------------------

User(s) arein group 'foo', IPSEC and WebVPN are selected as the tunneling protocol with a
30 minute idle timeout, Simultaneous Logins (5000)  ESP-3DES-MD5 and store password
on client is permitted (when using the software client, authenticating user is prompted by
the VPN software client on the PC)

vpn2-3080-1: IKE Proposals -> 1

                           The Active IKE Proposals
-------------------------------------------------------------------------------
| 1. IKE-3DES-MD5                      | 2. IKE-3DES-SHA                      |
-------------------------------------------------------------------------------
```

In testing the userid of **aprilmay**, the configured password is entered when prompted for this information by the Cisco VPN client. The group name **foo** and group key are configured in the client software along with the destination IP address of the concentrator, 10.81.7.57 and IPSec/UDP is defined as the transport.

Summary

This section addresses the need to provide secure, authenticated, network access from the enterprise network and the public Internet to the video surveillance VRF for real-time viewing of surveillance feeds. One method of accomplishing this is through the use of a VPN concentrator that can be accessed by appropriately configured workstations. This technique extends access to the segemented and logically isolated video surveillance deployment from any location with sufficient bandwidth to view the video feed.

References

The concepts in this document are intended to be focused on a targeted deployment for implementing IP video surveillance at the branch and central command center campus with controlled access from the enterprise network. For additional deployment information and a more thorough discussion of these concepts, refer to the following documents:

- *Network Virtualization—Path Isolation Design Guide Network Virtualization 3.0 - CVD*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html

- *Ethernet Access for Next Gen Metro and Wide Area Networks*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Ethernet_Access_for_NG_MAN_WAN_V3.1_external.html

- Other relevant Cisco Validated Design (CVD) design guides, refer to the following URL:

  www.cisco.com/go/designzone