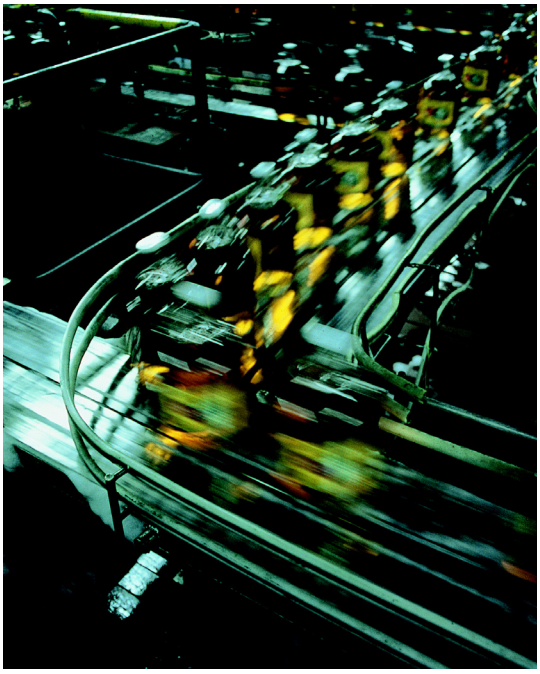


Site-to-Site VPN to a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

March 2016

Cisco Validated Design

Document Reference Number: ENET-TD012A-EN-P

Preface

The Site-to-Site Virtual Private Network (VPN) to a Converged Plantwide Ethernet (CPwE) Architecture Cisco Validated Design (CVD), which is documented in this Design and Implementation Guide (DIG), outlines application use cases for connecting remote Industrial Automation and Control System (IACS) assets to a plant-wide network architecture. This DIG highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the framework of CPwE.

Note CPwE CVD architectures are implemented, tested and validated to help ensure functionality and performance. In this CVD, the Allen-Bradley® Stratix 5900™ Service Router was used as the remote site router and a single Cisco ASR-1004 DMVPN hub router was used at the main site. The Stratix 5900 supports Pre-Shared Keys (PSKs), but it does not support certificate-based authentication. If the remote site security policies require certificate-based authentication, it is recommended that a suitable Cisco Integrated Service Router (ISR) replacement be used for the design.

Note This release of the CPwE architecture focuses on EtherNet/IP™, which uses the ODVA Common Industrial Protocol (CIP™) and is ready for the Industrial IoT. For more information on EtherNet/IP, see odva.org at the following URL:

- http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

For More Information

More information on CPwE Design and Implementation Guides can be found at the following URLs:

- Rockwell Automation® site:
  - http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page?#Whitepapers
- Cisco site:
  - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Target Audience

This DIG addresses applications that require connectivity between remote sites with IACS assets back to a main plant site for the purpose of supporting, monitoring, and maintaining the remote sites. This Site-to-Site VPN CPwE architecture helps plant personnel or other IACS assets within the plant Industrial Zone connect to a remote site. The Site-to-Site VPN CPwE design uses secure Internet Protocol (IP) VPNs to provide the primary network transport for a remote site.

The target audience for this DIG are network designers, Industrial Information Technology (IT), Enterprise IT, or other personnel who are comfortable with the following technologies:

- Industrial Demilitarized Zone (IDMZ)
- Routing and routing protocols
- Wide Area Network (WAN) and Internet Service Provider (ISP)
- IPsec and Generic Routing Encapsulation (GRE) fundamentals
- Cisco Command Line Interface (CLI)

Note For more information about IDMZ methodologies and designs, see the *Securely Traversing Industrial Automation Control System (IACS) Data Across the Industrial Demilitarized Zone Design and Implementation Guide* at the following URLs:

Rockwell Automation Site:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

Cisco Site:

- http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/WP/CPwE_IMDZ_WP/CPwE_IMDZ.html

Document Organization

The Site-to-Site VPN for a Converged Plantwide Ethernet Architecture DIG contains the following chapters and appendices:

Chapter or Appendix	Description
Site-to-Site VPN to a Converged Plantwide Ethernet Architecture Overview	Provides the Dynamic Multipoint Virtual Private Network (DMVPN) overview and use case requirements.
Site-to-Site Dynamic Multipoint Virtual Private Network Design	Provides the design overview of the DMVPN from a main site to a remote site.
Dynamic Multipoint Virtual Private Network Site-to-Site Configurations	Description of how to configure the DMVPN hub routers, the Enterprise and IDMZ firewalls, and the remote site #1 and 2 spoke routers.
References	List of references for CPwE and other concepts discussed in this document.
Test Hardware and Software	List of hardware and software components used in validation of this CVD.
Acronyms and Initialisms	List of acronyms and initialisms used in this document.

CHAPTER 1

Site-to-Site VPN to a Converged Plantwide Ethernet Architecture Overview

This chapter includes the following major topics:

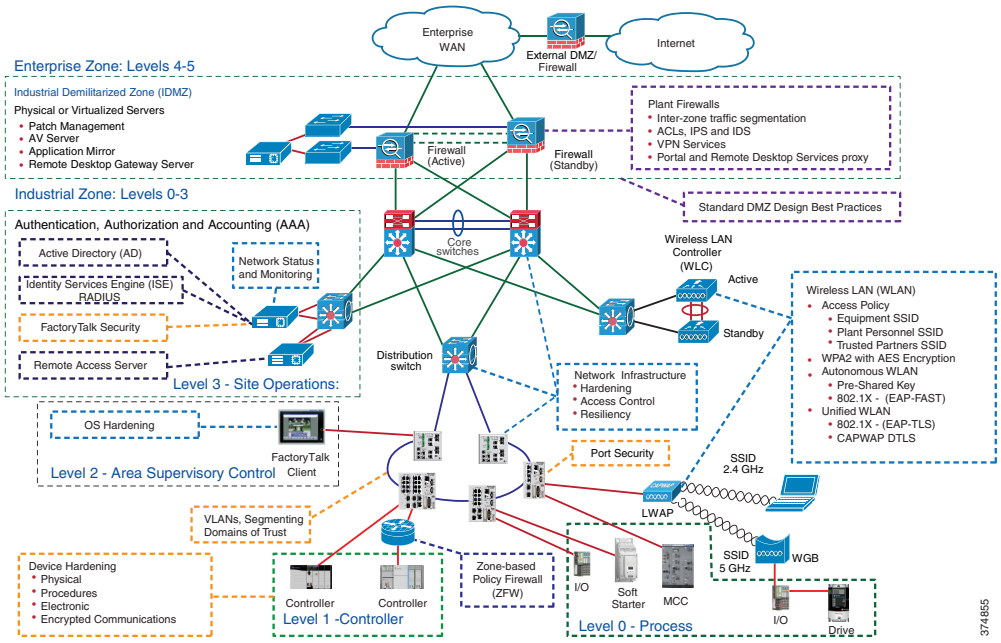
Business practices, corporate standards, industry standards, security policies and tolerance to risk are key factors in determining the design considerations and architectures required for secure site-to-site communications between a remote site and a plant-wide architecture.

Industrial Automation and Control System (IACS) networks are generally open by default. Openness facilitates both technology coexistence and IACS device interoperability. Openness also requires that IACS networks be secured by configuration and architecture-that is, defend the edge. Many organizations and standards bodies recommend segmenting business system networks from plant-wide networks by using an Industrial Demilitarized Zone (IDMZ).

The IDMZ exists as a separate network located in a level between the Industrial and Enterprise Zones, commonly referred to as Level 3.5. An IDMZ environment consists of numerous infrastructure devices, including firewalls, VPN servers, IACS application mirrors, remote gateway services, and reverse proxy servers, in addition to network infrastructure devices such as routers, switches, and virtualized services.

Converged Plantwide Ethernet (CPwE) is the underlying architecture that provides standard network services for control and information disciplines, devices, and equipment found in modern IACS applications. The CPwE architecture provides design and implementation guidance that can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of the IACS. The CPwE Industrial Network Security Framework (Figure 1-1) illustrates a holistic defense-in-depth approach, with multiple layers of security, applied at different levels of the CPwE architecture.

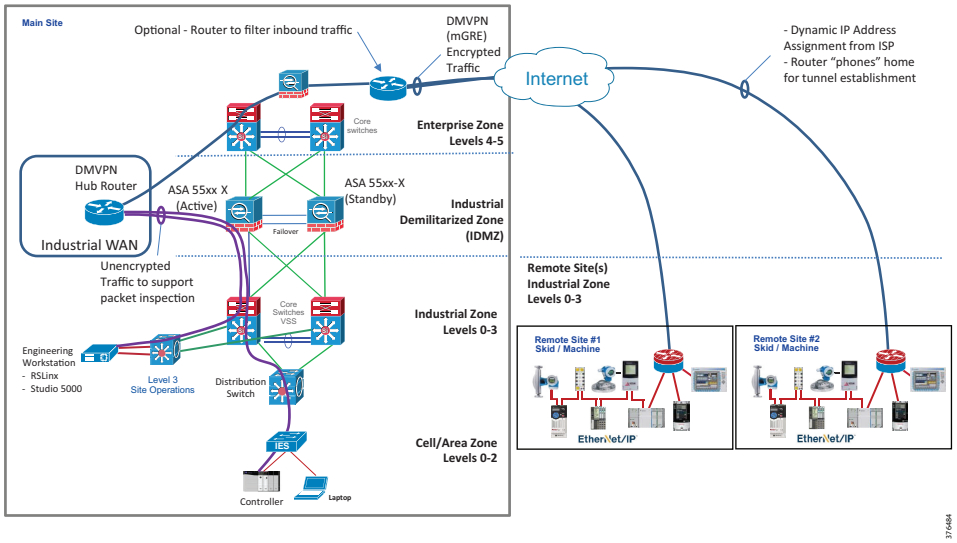
Figure 1-1 CPwE Industrial Network Security Framework



This Site-to-site VPN to CPwE CVD, which is brought to market through a strategic alliance between Cisco Systems® and Rockwell Automation, highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of site-to-site VPN use cases within the framework of CPwE.

Some IACS applications having multiple sites to support, monitor and maintain have adopted VPN technologies to connect their main plant sites to their remote sites or have used this technology to connect multiple campuses together. This DIG provides design and deployment considerations to help configure a site-to-site VPN connection between the main plant site Industrial WAN Zone and remote sites that contain an Allen-Bradley Stratix 5900 Service Router.

Figure 1-2 Site-to-Site VPN via Industrial WAN Architecture



Several architectures were considered during the development of this CVD, but this DIG highlights the design and deployment considerations to help with the creation of an Industrial WAN Zone that connects into the IDMZ firewalls as a boundary security appliance. The Industrial WAN Zone is a security zone, separate from the IDMZ, where remote industrial site(s) connect to the main site via DMVPN. The Industrial WAN security zone was created to:

- Act as a consolidated VPN termination end point for all remote sites
- Provides a zone for unencrypting traffic from the remote sites to allow traffic inspection if required
- Allow for separation of duties between IDMZ and Industrial WAN administrators
- Support separation of Industrial WAN policies from other security zones
- Separate Enterprise WAN traffic from Industrial WAN traffic

This CVD connected the Industrial WAN Zone to the Enterprise firewall as the connection point to the Internet. It also connected to the IDMZ firewalls as the connection point to the Industrial Zone. This DIG used a single Aggregation Service Router (ASR) that supported DMVPN in the Industrial WAN.

This DIG is predicated on an ISR, such as the Stratix 5900, with Zone-Based Policy Firewall (ZFW) located at the remote site. This architecture will typically be beneficial to users who support remote locations that contain a small numbers of IACS devices; such as, Programmable Automation Controllers (PACs), Variable Frequency Drives (VFDs), and Human Machine Interfaces (HMIs).

This Site-to-Site VPN to CPwE CVD tested and validated the following use cases for Industrial Zone, to Industrial WAN, to a remote site via VPN technologies:

- Studio 5000 Logix Designer® software on-line edit, upload, download
- RSLinx® Classic software *RSWho* functionality
- ControlLogix® controller messages
- Remote Desktop

DMVPN Overview

This Site-to-site VPN to CPwE CVD architecture uses the Internet for WAN transport. For data security and privacy concerns any site-to-site traffic that traverses the Internet must be encrypted. Multiple technologies can provide encryption, but the method that provides the best combination of performance, scale, application support, and ease of deployment is DMVPN.

The single-link use cases in this DIG use Internet/DMVPN as a primary WAN transport that requires a DMVPN single-cloud, single-hub design. The DMVPN routers use tunnel interfaces that support IP unicast as well as IP multicast and broadcast traffic, including the use of dynamic routing protocols.

Note GRE was chosen for this CVD in order to support use cases that needed IP multicast such as routing protocols or other applications. It is not recommended to use IP multicast for EtherNet/IP Controller-to-I/O communications through the GRE tunnel.

It is common for a firewall to be placed between the DMVPN hub routers and the Internet. In many cases, the firewall may provide Network Address Translation (NAT) from an internal RFC-1918 private IP address (such as 172.24.1.4) to an Internet-routable public IP address. The DMVPN solution works well with NAT, but requires the use of IPsec transport mode to support a DMVPN hub behind static NAT.

DMVPN requires the use of Internet Security Association and Key Management Protocol (ISAKMP) keep alive intervals for Dead Peer Detection (DPD), which is essential to facilitate fast reconvergence and for spoke registration to function properly in case a DMVPN hub is reloaded. This design helps enable a spoke to detect that an encryption peer has failed and that the ISAKMP session with that peer is stale, which then allows a new one to be created. Without DPD, the IPsec SA must time out (the default is 60 minutes) and when the router cannot renegotiate a new SA, a new ISAKMP session is initiated. The maximum wait time is approximately 60 minutes.

One of the key benefits of the DMVPN solution is that the spoke routers can use dynamically assigned addresses, often using Dynamic Host Configuration Protocol (DHCP) from an Internet Provider. The spoke routers can leverage an Internet default route for reachability to the hub routers and also other spoke addresses.

The DMVPN hub routers have static IP addresses assigned by the Internet Service Provider (ISP) to their public-facing interfaces. This configuration is essential for proper operation as each of the spoke routers have these IP addresses embedded in their configurations.

More information on hub-and-spoke router concepts can be found at the following URL:

- http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/prod_presentation0900aecd80313c9d.pdf

This DIG is predicated on a wired connection from the Stratix 5900 to the ISP; wireless, cellular, or satellite connectivity is not addressed as part of this CVD.

Use Case Requirements

The use case requirements are outlined as follows:

1. Help allow a main plant site user to securely connect to a remote site PAC using Studio 5000 Logix Designer for on-line edits, upload, and download programs.
2. Help enable centralized data collection and monitoring of the IACS application at the remote site.
3. Help simplify remote site maintenance by allowing consistent and repeatable remote site deployments including IACS control and information applications and IP addresses.
4. Help allow the main plant site user to connect to a remote desktop at the remote site.
5. Help use technology that helps enable converged IACS applications such as alarm systems and IP video surveillance.
6. Helps secure encrypted communications for up to 100 multiple locations.

CHAPTER 2

Site-to-Site Dynamic Multipoint Virtual Private Network Design

This chapter provides the design overview of the Dynamic Multipoint Virtual Private Network (DMVPN) from a main site to a remote site. It will describe the architecture, objectives, and main design principles of the Site-to-Site VPN solution. For more complex deployments, Cisco and Rockwell Automation recommend the involvement of Enterprise IT networking experts, or external resources such as an ISP, Cisco, or Rockwell Automation networking services.

This chapter includes the major following topics:

Design Overview

Discrete and process manufacturing companies that are geographically dispersed often require connectivity between sites. These types of organizations rely on the Wide Area Network (WAN) to provide sufficient performance and reliability for main site users to be effective in supporting remote site locations.

The CPwE and the CPwE IDMZ for IACS applications document present best practices for the Industrial Zone network and security architectures. These documents show the Industrial Zone being separated from the Enterprise Zone by means of the IDMZ, but do not address the connectivity of remote sites into the main site Industrial Zone. Remote IACS sites that must be maintained by personnel in the Industrial Zone can be thought of as extensions to the Industrial Zone.

The design presented in this CVD explains how to connect these remote sites into the main site's Industrial Zone via an Industrial WAN Zone, as shown in Figure 1-2 on page 1-2. It also explains how to establish a VPN tunnel between the main site and the remote site using GRE over IPsec. These two technologies are used to establish encrypted communications between the main and remote sites.

Note Other WAN architectures and technologies such as Multiprotocol Label Switching (MPLS) are not discussed in this CVD, but can be found in the *Cisco VPN WAN Technology Design Guide* at the following URL:

- http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf

While Internet IP VPN networks present an attractive option for effective WAN connectivity, any time an organization sends data across a public network, compromised data is a risk. Loss or corruption of data can result in a regulatory violation and can present a negative public image, either of which can have significant financial impact on an organization. Secure data transport over public networks like the Internet requires adequate encryption to protect business information.

This CVD helps organizations connect remote sites over public cloud Internet services and secure communications between sites. It also enables the following network capabilities:

- Secure, encrypted communications for Internet-based WAN solutions for multiples locations by using a hub-and-spoke architecture.
- Network Address Translation (NAT) implemented at the Enterprise firewall and remote site spoke router. This provides public-to-private IP address translations for the main and remote site(s).

Note Securing remote site(s) to meet a corporate or formalized standard is beyond the scope of this CVD. This CVD provides guidance for establishing DMVPN communications between a main site and remote site(s). Security policies for remote site(s) should be considered during the DMVPN design and implementation phases.

Generic Routing Encapsulation Protocol over IPsec

Network connectivity from the main site Industrial Zone is accomplished by establishing a VPN tunnel between the Industrial WAN VPN hub router(s) and the remote site spoke routers. This is further accomplished by using IPsec for the VPN tunnel creation and data encryption. GRE is used to encapsulate the data that traverses the VPN tunnel because of its flexibility to encapsulate many types of traffic that cannot be supported by IPsec alone. This section describes attributes and features of IPsec and GRE.

IPsec

The IPsec standard provides a method to manage authentication and data protection between multiple cryptographic peers engaging in secure data transfer. IPsec is an IP security feature that provides robust authentication, integrity, and encryption of IP packets between two or more participating peers.

IPsec uses symmetrical encryption algorithms for data protection, which is more efficient and easier to implement in hardware. These algorithms need a secure method of key exchange to help ensure data protection so Internet Key Exchange (IKE) protocols provide this capability.

IPsec provides encryption against eavesdropping and a choice of authentication algorithms to help ensure the data has not been altered and the data is from the trusted source.

The IPsec standard includes two IP protocols for encryption and authentication:

- Encapsulating Security Protocol (ESP)

- Authentication Header (AH)

ESP provides packet encryption and optional data authentication and anti-replay services while AH provides data authentication and anti-replay services, but no encryption. This CVD uses the ESP implementation because encryption for data privacy was required.

IPsec Transport Mode

IPsec has two modes of forwarding data across a network:

- Tunnel mode
- Transport mode

IPsec tunnel mode encrypts the source and destination IP addresses of the original packet, and a new IP header is added so that the packet can be successfully forwarded. This mode is not used when another tunneling protocol like GRE is used.

IPsec transport mode is usually used when another tunneling protocol like GRE is used, which is the case in this CVD. GRE is used to first encapsulate the IP data packet and then IPsec is used to protect the GRE tunnel packets. This CVD used IPsec transport mode to support using GRE.

IPsec transport mode works by inserting the ESP header between the IP header and the GRE protocol header. Since both IP addresses of the two GRE network nodes are visible in the IP header of the post-encrypted packet, they can be susceptible to traffic analysis attacks. By using GRE over IPsec, this design hides the addresses of the end stations by adding the encrypting the original IP header. See Figure 2-1 on page 2-4.

NAT and Port Address Translation (PAT) can be used with transport mode and DMVPN requires transport mode when there is a NAT device in between hub and spoke.

Note For additional information concerning DMVPN and IPsec transport mode, see *Dynamic Multipoint VPN* at the following URL:

- http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-2mt/sec-conn-dmvpn-dmvpn.html#GUID-D8F6839F-D735-4C8E-A199-602CDD8F7DD0

Generic Routing Encapsulation

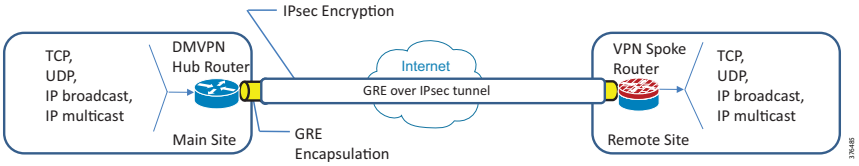
Although IPsec helps provide a secure method for tunneling data across an IP network, it is limited. IPsec does not support IP broadcast or IP multicast, preventing the use of protocols, such as routing protocols, which rely on these features. IPsec also does not support the use of multiprotocol traffic.

GRE is a protocol that can be used to *carry* other passenger protocols, such as IP broadcast or IP multicast, as well as non-IP protocols.

Note GRE was chosen for this CVD to support use cases that needed IP multicast such as routing protocols or other applications. It is not recommended to use IP multicast for EtherNet/IP Controller-to-I/O communications through the GRE tunnel.

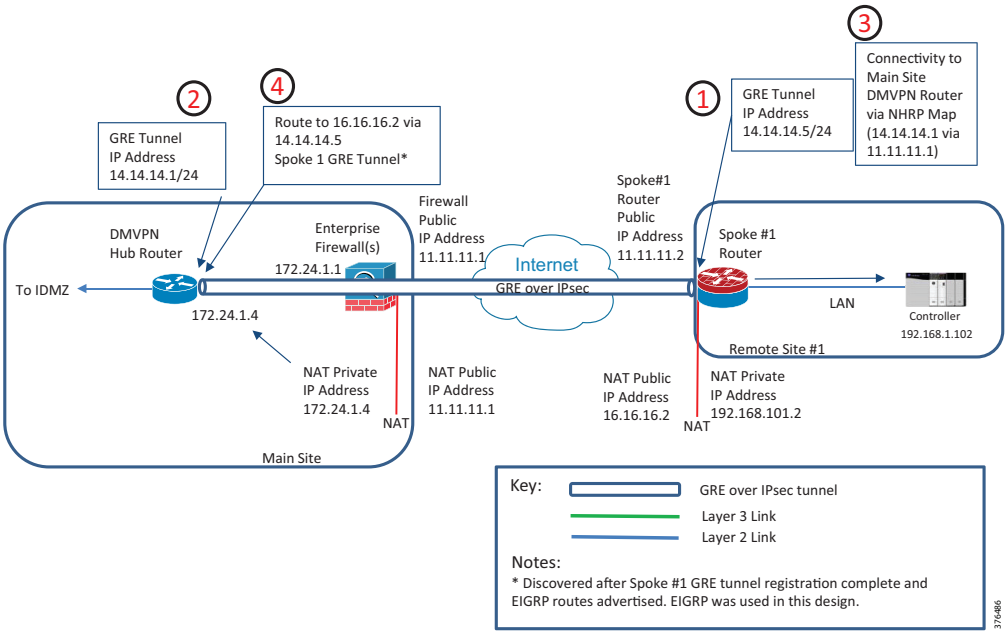
Using GRE tunnels in conjunction with IPsec provides the ability to run a routing protocol with encrypted data across an unsecured network between the main and remote sites. See Figure 2-1.

Figure 2-1 GRE for Protocol Encapsulation and IPsec for Security



In this CVD, GRE tunnels are configured with their own IP address as shown in Figure 2-2, call-out bubbles #1 and #2, in order to identify the tunnel. The Spoke #1 router will register with the main site DMVPN router in order to build the GRE over IPsec tunnel.

Figure 2-2 GRE and Routing via Next Hop Routing Protocol

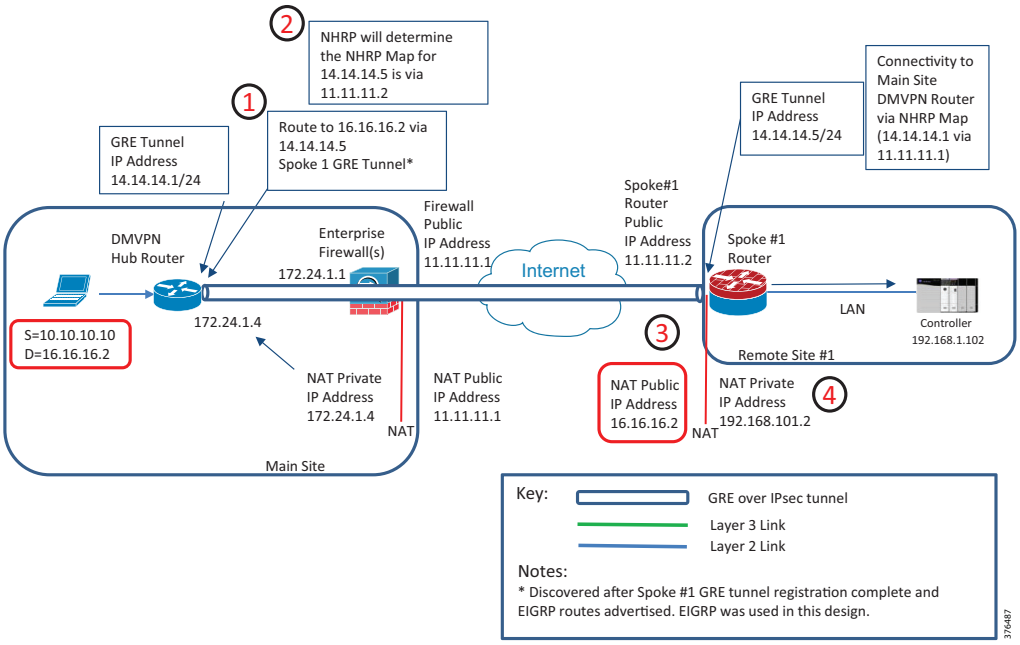


GRE encapsulates the data and uses the Next Hop Router Protocol (NHRP) to determine the route from the remote site to the main site DMVPN hub router. The next hop router is defined in the remote site tunnel configuration to identify the IP address of the main site GRE tunnel and the IP address of the interface that can reach the other end of the tunnel. (See Figure 2-2, call-out bubble #3.)

Once the Spoke #1 router is connected to the Internet, the Spoke #1 router will attempt to establish the GRE tunnel by sending the registration request to the main site DMVPN hub router. Once the tunnel is created, the main site router and remote site router will be able to communicate through the GRE over IPsec tunnel. Once the DMVPN tunnel is established the EIGRP routes are advertised, the main site DMVPN router will contain the route to the remote site networks. (See Figure 2-2, call-out bubble #4)

This DIG has briefly covered discussed how GRE and IPsec work together to encapsulate and encrypt the traffic between the main site and the remote site. In Figure 2-3, we show an example of a host at the main site with an IP address 10.10.10.10 attempting to reach a remote site IP address of 16.16.16.2, which represents the public NAT-translated IP address of the controller at 192.168.1.102.

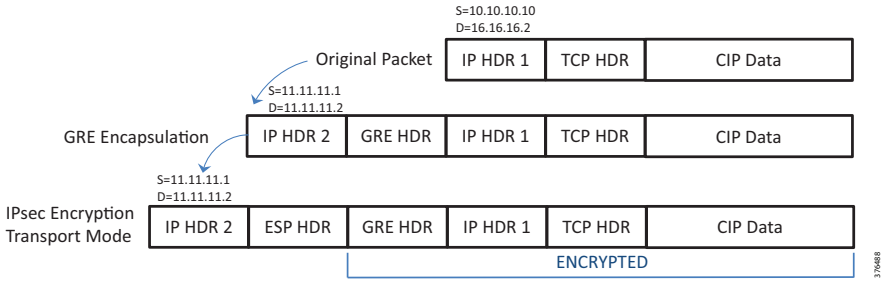
Figure 2-3 Main Site to Remote Site GRE over IPsec Example



We see from Figure 2-3, call-out bubble #1, that once the GRE tunnel is established and the remote site networks are advertised, the route to 16.16.16.2 will be via the GRE tunnel. NHRP will determine that the best way to reach the remote site GRE tunnel is via the remote site 11.11.11.2 physical interface, call-out bubble #2.

Figure 2-4 is a high level representation of how an IP packet is encapsulated by GRE and encrypted by IPsec and matches the above example.

Figure 2-4 GRE and IPsec Packet Diagram



Once the packet reached the end of the GRE tunnel at the Spoke #1 router, the packet is de-encapsulated and unencrypted. A one-to-one (1:1) NAT is configured on the Spoke #1 router so the IP addresses of the remote site controller could remain the same at each remote site. A public IP address of 16.16.16.2 is NAT-translated to 192.168.1.102.

Virtual Route Forwarding and Front Door Virtual Route Forwarding

Virtual Route Forwarding (VRF) is a technology used in computer networks that allows multiple instances of a routing table to co-exist within the same router. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

VRFs are also used in conjunction with GRE solutions to:

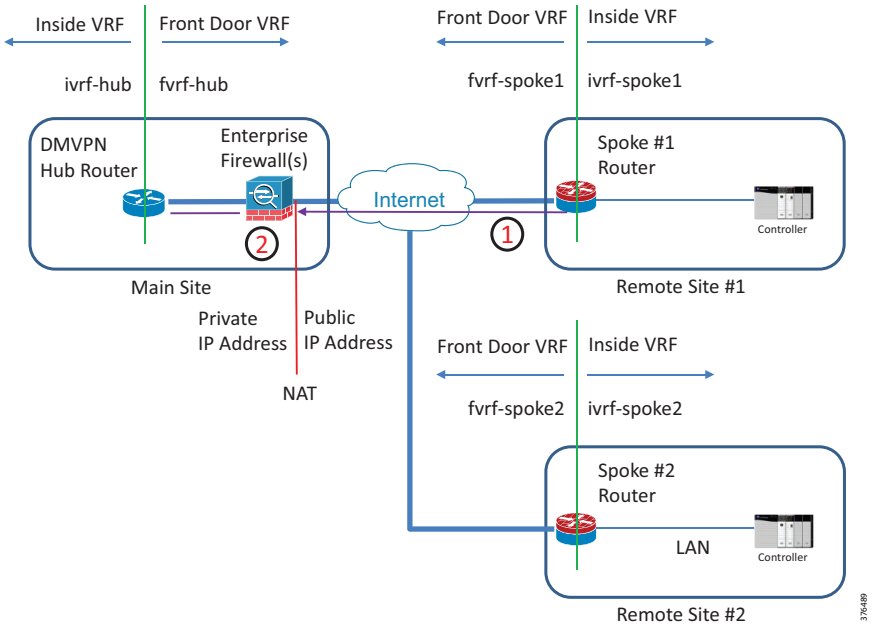
- Keep the routing information for tunnel establishment separate from the routing information for IACS communication and other remote site traffic
- Force the remote-site tunnel establishment to be resolved in the VRF specified instead of the default, global routing table

A router can have multiple routing tables that are kept logically separate on the device. This separation is similar to a virtual router from the forwarding plane perspective. The global VRF corresponds to the traditional routing table, and additional VRFs are given names and Route Descriptors (RDs). Certain features on the router are VRF aware, including static routing and routing protocols, interface forwarding, and IPsec tunneling. This set of features is used in conjunction with DMVPN to permit the use of multiple default routes for both the DMVPN hub routers and DMVPN spoke routers. This combination of features is referred to as Front-door Virtual Route Forwarding (FVRF) because the VRF faces the Internet and the router internal interfaces and the Multipoint Generic Routing Encapsulation (mGRE) tunnel all remain in the global VRF.

The IP routing policy used in this design for the WAN remote sites does not allow direct Internet access for web browsing or other uses by any remote-site hosts. Internet access from a remote site host must do so via the Internet edge at the primary site. The end hosts require a default route for all Internet destinations; however, this route must force traffic across the primary WAN transport DMVPN tunnel.

In this CVD, the FVRF's IP addresses are used to establish the GRE tunnel endpoints. See Figure 2-5.

Figure 2-5 Front Door VRF



As a remote site spoke router is commissioned, the spoke router will communicate from the FVRF interface to the public IP address of the Enterprise firewall as shown above in call-out bubble #1 in Figure 2-5.

The Enterprise firewall using NAT will forward the traffic to the VPN hubs FVRF IP address as shown in call-out bubble #2 in Figure 2-5.

Enhanced Interior Gateway Routing Protocol Routing

This CVD used Enhanced Interior Gateway Routing Protocol (EIGRP) as the primary routing protocol because it is easy to configure, does not require a large amount of planning, has flexible summarization and filtering, and can scale to large networks.

Some of the many advantages of EIGRP are:

- Very low usage of network resources during normal operation; only hello packets are transmitted on a stable network
- When a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load the routing protocol itself places on the network
- Rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous)

In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic.

Encryption

The primary goal of encryption is to help provide data confidentiality, integrity, and authenticity by encrypting IP packets as the data travels across a network.

The encrypted payloads are then encapsulated with a new header (or multiple headers) and transmitted across the network. The additional headers introduce a certain amount of overhead to the overall packet length. The packet overhead associated with encryption based on the additional headers required for various combinations of IPsec and GRE is 60 bytes.

A Maximum Transmission Unit (MTU) parameter exists for every link in an IP network; typically, the MTU is 1500 bytes. IP packets larger than 1500 bytes must be fragmented when transmitted across these links.

Fragmentation is not desirable and can impact network performance. To avoid fragmentation, the original packet size plus overhead must be 1500 bytes or less, which means that the sender must reduce the original packet size. To account for other potential overhead, this CVD recommends that tunnel interfaces with a 1400 byte MTU are configured.

The Maximum Segment Size (MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. The MSS value is sent as a Transmission Control Protocol (TCP) header option only in TCP Synchronization (SYN) segments. Each side of a TCP connection reports its MSS value to the other side. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

The IP and TCP headers combine for 40 bytes of overhead, so the typical MSS value reported by network clients will be 1460. This design includes encrypted tunnels with a 1400 byte MTU, so the MSS used by endpoints should be configured to be 1360 to help minimize any impact of fragmentation.

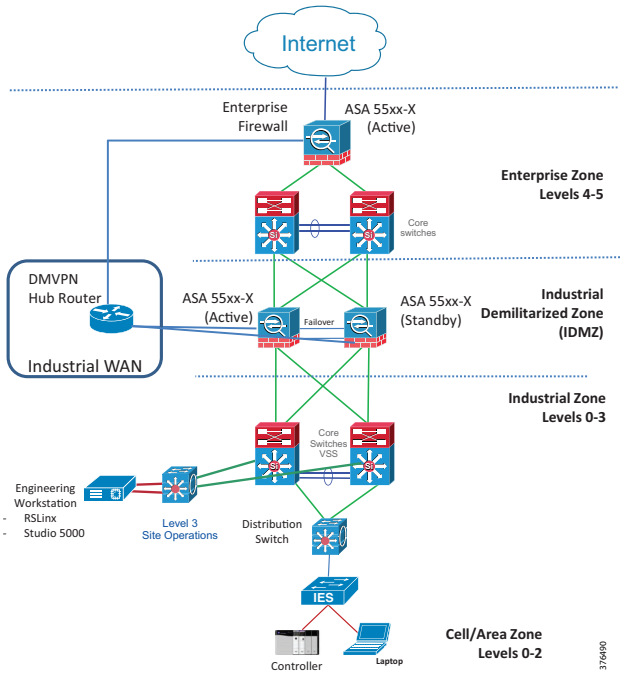
IPsec Security Association (SA) anti-replay is a security service in which the decrypting router can reject duplicate packets and protect itself against replay attacks. Cisco IOS provides anti-replay protection against an attacker duplicating encrypted packets. By expanding the IPsec anti-replay window, the router can be allowed to keep track of more than the default of 64 packet.

Wide Area Network Design Considerations

The primary focus of this CVD design is to allow use of Internet VPN, which is a commonly deployed WAN transport for both primary and secondary links. At a high level, the WAN is an IP network, and this transport can be easily integrated to the design. The chosen architecture designates a primary WAN aggregation site that is analogous to the hub site in a traditional hub-and-spoke design.

This CVD tested one primary WAN connection from the Internet connected to the Enterprise firewall, as shown in Figure 2-6.

Figure 2-6 Single Internet Connection



Note For additional WAN CVD guidelines, see the *Cisco VPN WAN Technology Design Guide* at the following URL:

- http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf

Internet as WAN Transport

The Internet is essentially a large-scale public WAN composed of multiple interconnected service providers. The Internet can provide reliable high-performance connectivity between various locations, although it lacks any explicit guarantees for these connections. Despite its *best effort* nature, the Internet is a sensible choice for a primary transport when it is not feasible to connect with another transport option. Additional resiliency can be provided by using the Internet as an alternate transport option.

Internet connections are typically included in discussions relevant to the Internet edge, specifically for the primary site. Remote site routers also commonly have Internet connections, but do not provide the same breadth of services using the Internet. For security and other reasons, Internet access at remote sites is routed through the primary site.

Dynamic Multipoint Virtual Private Network

DMVPN is a Cisco solution for building scalable site-to-site VPNs that supports a variety of applications. DMVPN uses the following protocols to provide the hub to spoke communications:

- IPsec for encryption
- mGRE for data encapsulation
- NHRP for mapping database of all the spoke tunnels to real (public interface) addresses

DMVPN is widely used for encrypted site-to-site connectivity over public or private IP networks and can be implemented on all WAN routers used in this CVD. It supports on-demand full mesh connectivity with a simple hub-and-spoke configuration. DMVPN was also used in this CVD because it supports spoke routers that have dynamically assigned IP addresses.

DMVPN makes use of mGRE tunnels to interconnect the hub to all of the remote site spoke routers. This technology combination supports unicast, multicast, and broadcast IP, including the ability to run routing protocols within the tunnels.

Note GRE was chosen for this CVD to support use cases that needed IP multicast such as routing protocols or other applications. It is not recommended to use IP multicast for EtherNet/IP Controller-to-I/O communications through the GRE tunnel.

Ethernet Wide Area Network

The WAN transports mentioned previously use Ethernet as a standard media type. Since Ethernet is becoming a dominant carrier hand off in many markets, it was included as the primary media in the tested and validated CPwE architectures.

Wide Area Network Aggregation Designs

WAN aggregation in the context of this CVD refers to connecting all the remote site spoke routers into the main site hub router(s) from an Internet transport. WAN routers that terminate VPN traffic at the main site are referred to as VPN hub routers.

This CVD differs from an Enterprise-only WAN design to the extent that it addresses the additional connectivity of the Industrial Zone within a discrete manufacturing or process plant. The VPN hub routers aggregate traffic from the remote site spoke routers behind an Enterprise firewall and connect to the Industrial Zone via either the IDMZ firewalls or through a separate pair of Industrial Zone Industrial WAN firewalls. In this CVD, only a single primary Internet link with two remote sites was tested for the WAN transport. This design is referred to as the DMVPN only design.

For the dual DMVPN design model that uses Internet VPN as both a primary and secondary transport, using dual Internet service providers can be architected, but was not tested and validated in this CVD. The various design models are contrasted in the Table 2-1.

Table 2-1 Design Models Using Only VPN Transport

	DMVPN Only Design Model	Dual DMVPN Design Model
Remote sites	Up to 100	Up to 500
WAN links	Single	Dual
DMVPN hubs	Single	Dual
Transport 1	Internet VPN	Internet VPN
Transport 2	-	Internet VPN

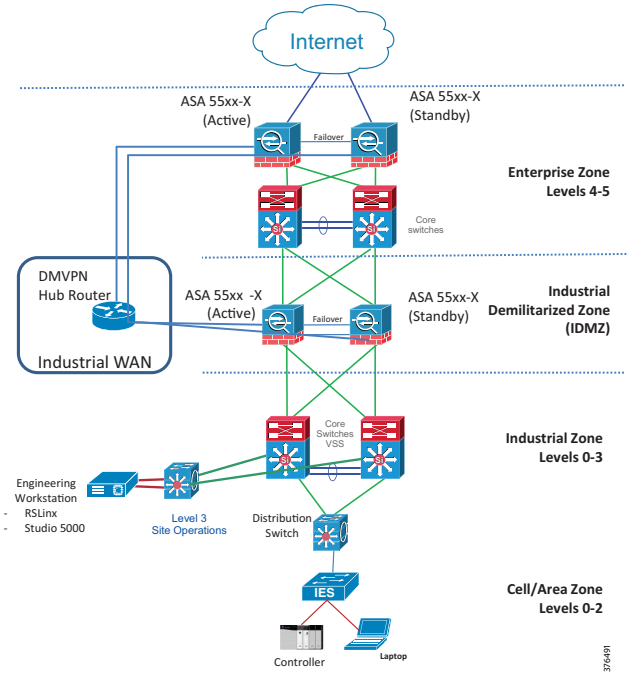
Note For further information about dual DMVPN designs, see the *Cisco VPN WAN Technology Design Guide* at the following URL:

- http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf

DMVPN Only Design Model

This CVD tested and validated a single ASR DMVPN hub router in the Industrial WAN Zone. The hub routers was connected to the Enterprise firewall(s), which were connected to the Internet. The DMVPN hub routers provided connectivity to the Industrial Zone through interfaces on the IDMZ firewalls. See Figure 2-7.

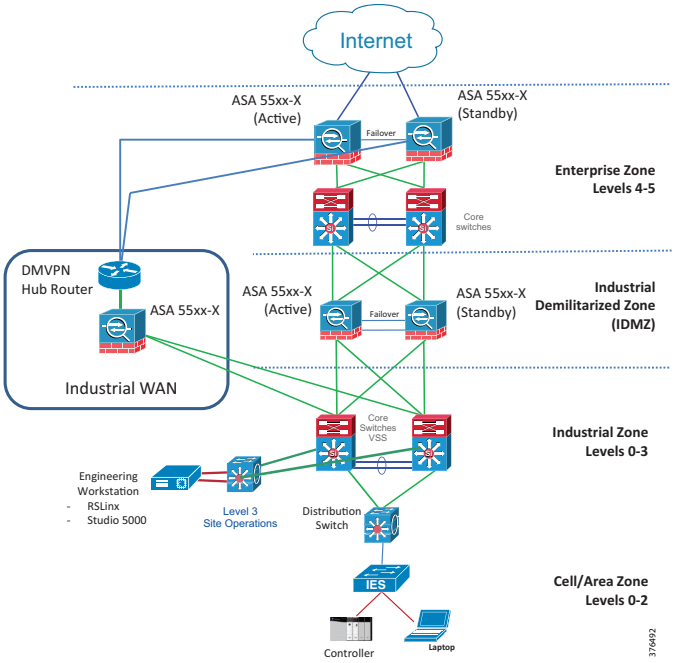
Figure 2-7 DMVPN Only Design Model Connected to IDMZ Firewalls



This tested and validated CPwE architecture is one of many possible solutions to connect the Industrial WAN into the Industrial Zone.

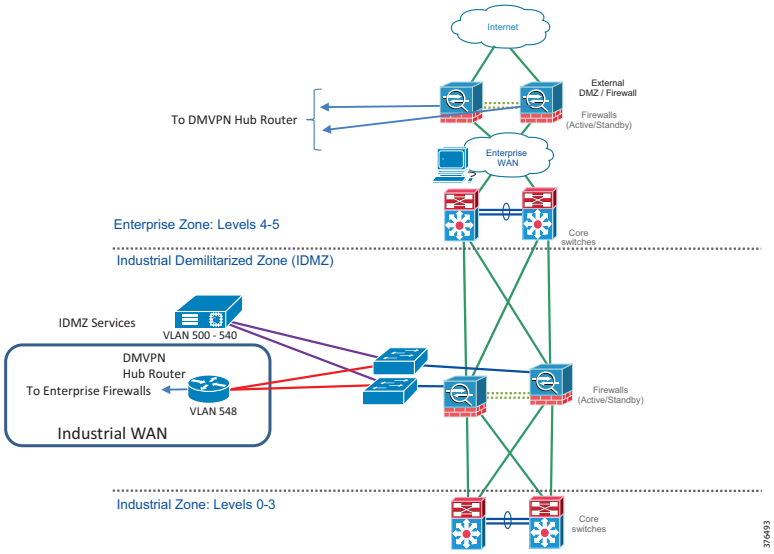
It is also possible to architect this solution (not part of this CVD) with separate Industrial WAN firewalls to keep the Industrial WAN traffic separate from the IDMZ. See Figure 2-8. Some organizations, depending on their security stance, may prefer to separate the Industrial WAN logically and physically for organizational reasons (such as one department being responsible for the WAN but not for the IDMZ or Industrial Zone assets). Separation may also be based on a security policy that helps maintain that an accidental misconfiguration of the WAN could adversely affect the IDMZ security.

Figure 2-8 DMVPN Only Design Model with Separate Industrial WAN Firewalls



A third option (not part of this CVD) for connecting the ASR hub routers is to use the IDMZ switches and add another IDMZ VLAN to separate the Industrial WAN traffic. See Figure 2-9.

Figure 2-9 DMVPN Only Design Model Using IDMZ Switches



In all of these architectures, the traffic between the VPN hub routers and IDMZ or Industrial WAN firewalls is unencrypted to support traffic inspection.

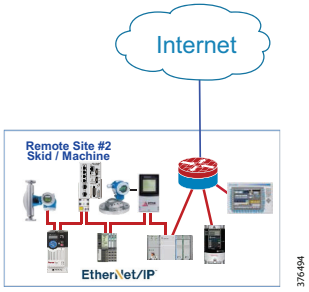
Wide Area Network Remote Site Designs

This DIG documents a single, non-redundant WAN remote site router design. See Figure 2-10.

Note For additional documented solutions, see the *Cisco VPN WAN Technology Design Guide* at the following URL:

- http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf

Figure 2-10 Non-Redundant Internet WAN Remote Site Design



Most remote sites are designed with a single router and single WAN connection. In this CVD, the following requirements were met through the presented design:

- IACS controller assets have the same IP address regardless of remote site location.
- Studio 5000® software will be used for online edits, upload, and download of IACS ControlLogix controllers.
- RSLinx *RSWho* functionality will be used to communicate with IACS ControlLogix controllers.
- ControlLogix controller message instructions will be used to communicate with between a main site ControlLogix controller and a remote site ControlLogix controller.
- Remote desktop technologies will be used to interact with a remote site computer.
- Remote site routers may have IP addresses assigned by an Internet Service Provider (ISP) using DHCP so therefore the IP address of the remote site may not be static.

Note Securing remote site(s) to meet a corporate or formalized standard is beyond the scope of this CVD. This CVD provides guidance for establishing DMVPN communications between a main site and remote site(s). Security policies for remote site(s) should be considered during the DMVPN design and implementation phases.

Wide Area Network/Local Area Network Interconnection

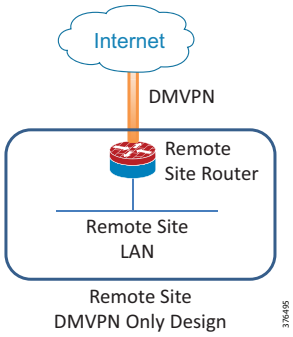
The primary role of the WAN is to interconnect the primary and remote-site LANs. The LAN discussion within this DIG is limited to how the DMVPN WAN hub router connects the remote site LANs into the Industrial Zone.

At remote sites, the LAN topology depends on the number of connected IACS devices and physical geography of the site. Large sites may require the use of a Distribution Layer to support multiple industrial Access Layer switches. Other sites may only require a single industrial Access Layer switch directly connected to the WAN remote-site routers. For testing purposes, the IACS devices were directly connected to the remote site spoke router.

Wide Area Network Remote Sites Local Area Network Topology

For consistency and modularity, all WAN remote sites used the same Virtual Local Area Network (VLAN) and IP subnet assignment scheme for the IACS network. See Figure 2-11.

Figure 2-11 WAN Remote Site-Flat Layer 2 LAN (Single Router)



WAN remote sites that do not require additional Distribution Layer routing devices are considered to be flat. In this design, all Layer 3 services are provided by the attached WAN router. The major advantage of this design is that all of the IACS devices can be configured identically, regardless of the number of sites in this configuration. In this DIG, VLAN 10 was configured in the remote site router and the IACS controller's default gateway was the IP address of VLAN 10. See Figure 2-12.

IP subnets are assigned on a per-VLAN basis. This design only allocates subnets with a 255.255.255.0 (/24) network mask for the Access Layer, even if fewer than 2534 IP addresses are required. (This model can be adjusted as necessary to other IP address schemes.)

For this CVD testing and validation, a single Rockwell Automation ControlLogix PAC was connected directly to the remote site router.

Remote Site Distribution and Access Layer

Large remote sites may require a LAN environment similar to that of a small campus LAN that includes a Distribution Layer and Access Layer. This topology can work well with either a single or dual router WAN edge. This CVD tested and validated a Stratix 5900 Service Router that provided the Distribution and Access Layer features within one device.

Note For details on how to implement a separate Distribution and Access Layer designs at the remote site, see the *Cisco VPN WAN Technology Design Guide* at the following URL:

- http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf

DMVPN Hub Routers

The DMVPN-only design is intended to support up to 100 remote sites with a combined aggregate WAN bandwidth of up to 1.0 Gbps. The most critical devices are the WAN routers that are responsible for reliable IP forwarding and Quality of Service (QoS). The amount of bandwidth required at the WAN aggregation site

determines which model of router to use. The choice of whether to implement a single router or dual router is determined by the number of DMVPN clouds that are required in order to provide connections to all of the remote sites.

Cisco Aggregation Services Router (ASR) 1000 Series represent the next-generation, modular, services-integrated Cisco routing platform. They are specifically designed for WAN aggregation. This CVD was tested and validated with a Cisco ASR-1004 as the DMVPN hub router.

Note For a list of Cisco-tested ASRs in the DMVPN architecture, see the *Cisco VPN WAN Technology Design Guide* at the following URL:

- http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf

Remote Sites DMVPN Spoke Router Selection

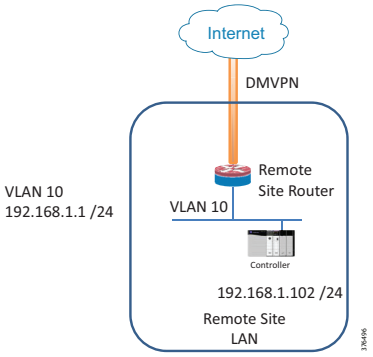
Many factors should be considered in the selection of the WAN remote site routers. Among those, and key to the initial deployment, is the ability to process the expected amount and type of traffic. An adequate number of interfaces and module slots, and a properly licensed Cisco IOS Software image that supports the set of features that is required by the topology must also be verified.

In this CVD, the Allen-Bradley Stratix 5900 was tested and validated as the remote site router. The Cisco 809 or 829 Industrial ISR could also be a consideration for a remote site router.

The DMVPN spoke routers at the remote sites connect to the Internet through a WAN interface. The single link DMVPN remote site is the most basic of building blocks for any remote location. This design can be used with the DMVPN spoke router connected directly to the Access Layer, or it can support a more complex LAN topology by connecting the DMVPN spoke router directly to a Distribution Layer. The design is such that the main site hub can communicate with each remote site router but remote site routers cannot directly communicate with each other. It is possible to design the DMVPN architecture to provide direct remote site to remote site communications, but it was not addressed nor desired in this design.

The IP routing is straightforward and can be handled entirely by static routes at the WAN aggregation site and static default routes at the remote site. However, configuring this type of site with dynamic routing can have considerable value. It is easy to add or modify IP networks at the remote site when using dynamic routing because any changes are immediately propagated to the rest of the network. See Figure 2-12.

Figure 2-12 DMVPN Remote Site (Single Link - Single Router)



The DMVPN connection can be the primary WAN transport, or it can also be the alternative to another DMVPN WAN transport. A DMVPN backup link can be added to an existing DMVPN single link design to help provide additional resiliency, either connecting on the same router or on an additional router. By adding a link, the first level of high availability for the remote site is provided. A failure in the primary link can be automatically detected by the router and traffic can be rerouted to the secondary path. It is mandatory to run dynamic routing when multiple paths exist. The routing protocols are tuned to help ensure the proper path selection.

The dual-router, dual-link design continues to improve upon the level of high availability for the site. This design can tolerate the loss of the primary router and traffic can be rerouted via the secondary router (through the alternate path).

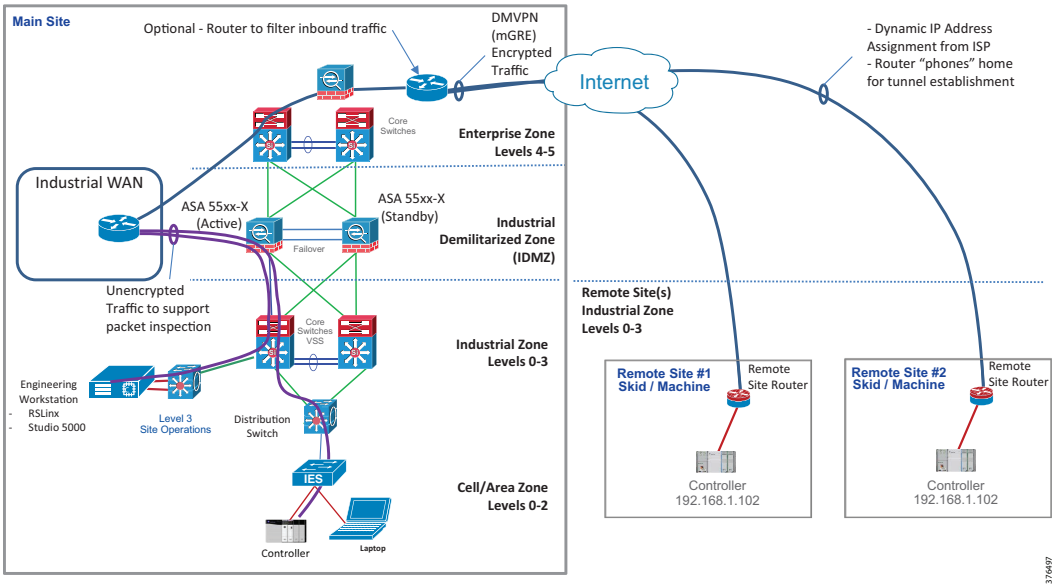
Note For more information on dual routers, dual link designs, see the *Cisco VPN WAN Technology Design Guide* at the following URL:

- http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf

Validated Design Details

The DMVPN hub routers connect to the Enterprise firewalls for connectivity to the Internet. The DMVPN routers also connect to the IDMZ firewalls to allow Industrial Zone users to have access to the remote sites. Figure 2-13 is a high level diagram with details of each major component described in the sections that follow.

Figure 2-13 DMVPN Architecture



Main Site DMVPN Hub Router

The DMVPN router uses a single connection to the Enterprise firewall and an EtherChannel consisting of a two port bundle to connect to the IDMZ firewalls. It must have sufficient IP routing information to provide end-to-end reachability. Maintaining this routing information typically requires a routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is used for this purpose.

The DMVPN hub routers use a FVRF named *fvrf-hub* with a static default route pointing to the Enterprise firewall interface. See Table 2-2.

Table 2-2 Example DMVPN Hub Router Addresses

Host Name	fvrf-hub IP address	EIGRP Process ID
ASR1-HUB	172.24.1.4/24	101

Main Site Enterprise Firewall

The main site Enterprise firewall was configured with a separate public interface to accept the remote site connections. This interface would be configured with a public IP address and the opening of two ports to accept IKE and NAT Traversal (NAT-T) traffic is required.

The IKE protocol defines a means of negotiation and authentication for IPsec SAs, which are security policies defined for secured communication between two or more entities such as between the remote site and main site routers. The IKE protocol helps to ensure security for SA establishment and uses port 500 for communication.

NAT-T is used if a NAT device, such as the Enterprise firewall, is placed between the remote site spoke route and the main site hub router. When a NAT device is used between the VPN client and the VPN headend, the NAT device can stop the VPN tunnel working because the port numbers get changed.

In order to get around this, NAT-T is used to encapsulate the IPsec in UDP packets with port 4500. This allows the NAT to modify the packet without breaking the IPSEC tunnel. NAT-T needs to be supported on the remote and main site routers.

Note To configure appropriate firewall rules, the design must include a list of expected traffic flows between the main and remote site(s). It is recommended that firewall rules be configured to deny all other unexpected traffic.

In this CVD, the ports shown in Table 2-3 were opened to permit the spoke-to-hub communications.

Table 2-3 Firewall Rules

Host Name	Spoke to Hub Interface IP Address	Allow the following UDP Ports	1:1 NAT
Enterprise Firewall	Dynamic or Set	500 - IKE, 4500 - NAT-T	Your Public IP address NAT-translated to 172.24.1.4 (Hub Router IP address)

The Enterprise firewall was also configured with a 1:1 NAT of the public IP address to the IP address of the DMVPN hub router.

Main Site IDMZ Firewall

The main site IDMZ firewall used a separate interface that was configured to accept traffic from the DMVPN hub routers. The firewall can be configured to support any expected protocols from the remote site, but in this CVD example, only CIP traffic and Remote Desktop Protocol were permitted to the remote sites.

Note To configure appropriate firewall rules, the design must include a list of expected traffic flows between the main and remote site(s). It is recommended that firewall rules be configured to restrict traffic to only specific source and destination IP addresses or subnets. It is also recommended to deny all other unexpected traffic.

It was assumed the DMVPN hub routers were connected to an existing IDMZ firewall. See Table 2-4.

Table 2-4 Enterprise Firewall Rules

Host Name	DMVPN Firewall Interface	Allow the following TCP and UDP Ports	1:1 NAT
IDMZ Active Firewall	Gi0/7	2222 UDP (CIP) 44818 TCP (CIP) 3389 TCP (RDP)	N/A
IDMZ Standby Firewall	Gi0/7	2222 UDP (CIP) 44818 TCP (CIP) 3389 TCP (RDP)	N/A

Remote Site DMVPN Spoke Router

The spoke routers were configured to establish a GRE tunnel to the main site hub router. This design assumes the IP address of the spoke routers Internet-facing interface may be dynamically assigned by the ISP or it may be statically set. The public IP address of the Enterprise firewall will be configured into the spoke router for GRE tunnel establishment.

Table 2-5 shows the example Enhanced Interior Gateway Routing Protocol (EIGRP) and NAT addresses used in the example.

Table 2-5 Example Spoke 1 and Spoke 2 Addresses

Host Name	Internet-facing IP address	fvrf-spoke1	EIGRP Process ID	1:1 NAT
Spoke1	Dynamic or Set	Assigned to Internet-facing Interface	101	Unique outside global address 16.16.16.2 NAT'ed to Inside local 192.168.1.102
Spoke2	Dynamic or Set	Assigned to Internet-facing Interface	101	Unique outside global address 15.15.15.2 NAT'ed to Inside local 192.168.1.102

In this CVD, the requirement to have a consistent ControlLogix PAC IP address at each remote site was accomplished by configuring a 1:1 NAT in the spoke router. This design, however, does require a unique global outside address at each remote site.

CHAPTER 3

Dynamic Multipoint Virtual Private Network Site-to-Site Configurations

This chapter describes how to configure the DMVPN hub routers, the Enterprise and IDMZ firewalls, and the Remote Site #1 and 2 spoke routers. The actual settings and values that are used are determined by organizational requirements and current network configuration. This CVD covers the basics of DMVPN connectivity configurations, but does not cover detailed security configurations.

This chapter includes the following major topics:

Note Security configurations for remote sites will vary based on the types of expected traffic from these sites and should be addressed on a site-by-site basis.

Configuring DMVPN Hub Router #1

This configuration has the following major steps:

1. Configuring the router host name
2. Setting the clock time zone
3. Creating the Front Door VRF
4. Creating the Inside VRF
5. Creating the Internet Security Association and Key Management Protocol for IPsec
6. Configuring the mGRE Tunnel Interface
7. Configuring the Enterprise and IDMZ-Connected Interfaces
8. Configuring Enhanced Interior Gateway Routing Protocol

9. Adding a Route to the Enterprise Firewall

Configure the Router Host Name

Enter global configuration mode and enter the DMVPN hub router #1's host name.

```
hostname ASR1-HUB
```

Set the Clock Time Zone

Set the clock time zone by entering the following commands. The configuration may vary based on location and time zone.

```
clock timezone EST -5 0
clock summer-time EDT recurring
```

Create the Front Door VRF

An Internet-facing VRF is created to support FVRF for DMVPN. The FVRF name in this CVD is *fvrf-hub*. An Associated RD must also be configured to make the FVRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the FVRF instance.

This design uses VRF Lite so that the RD value can be chosen arbitrarily, but it is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

The RD for this FVRF is 1:1.

```
ip vrf fvrf-hub
 rd 1:1
 route-target export 1:1
 route-target import 1:1
```

Create the Inside VRF

In this configuration, the inside VRF is named *ivrf-hub* and the RD for this VRF is 2:2.

```
ip vrf ivrf-hub
 rd 2:2
 route-target export 2:2
 route-target import 2:2
```

Create the Internet Security Association and Key Management Protocol for IPsec

Internet Security Association and Key Management Protocol (ISAKMP) policies can be configured for authentication from PSKs or digital certificates. This CVD used PSKs for the Stratix 5900 remote site spoke router due to limitations in the certificate support. If certificate support is required, it is recommended that a suitable Cisco platform is used as the remote site spoke router.

Step 1 Configure the crypto keyring.

The crypto keyring defines a PSK (or password) valid for IP sources that are reachable within a particular VRF. This key is a wildcard pre-shared key if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING vrf fvrf-hub
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 2 Configure the ISAKMP policy.

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by PSK
- Diffie-Hellman group: 2

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
```

Step 3 Create the ISAKMP Profile.

The ISAKMP profile creates an association between an identity address, a VRF, and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
   keyring DMVPN-KEYRING
   match identity address 0.0.0.0 fvrf-hub
```

Step 4 Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for this DMVPN example uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (Hash Message Authentication Code or HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
```

Step 5 Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

Step 6 Increase the IPsec anti-replay window size.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed. It is recommended that the maximum window size is used to minimize future anti replay problems. On the Cisco ASR 1000 router platform, the maximum replay window size is 512

If the window size is not increased, the router may drop packets and the following error message on the router CLI may display:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
crypto ipsec security-association replay window-size 512
```

Configure the mGRE Tunnel Interface

It is expected that multiple remote site spoke routers will connect to the main site DMVPN hub router. The mGRE tunnel interface in this example is used to connect to all remote sites.

For this CVD, the parameters show in Table 3-1 are used.

Table 3-1 DMVPN Hub Router #1 Configuring the mGRE Tunnel Interface Parameters

Device Host Name	Tunnel 0 IP address	IP address	EIGRP AS	NHRP Network ID
ASR-Hub1	14.14.14.1 /24	172.24.1.4	101	101

Enter global configuration mode and enter the following configuration for the DMVPN mGRE Tunnel 0.

```
interface Tunnel0
 ip address 14.14.14.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 101 35
 no ip next-hop-self eigrp 101
 no ip split-horizon eigrp 101
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp redirect
 tunnel source 172.24.1.4
 tunnel mode gre multipoint
 tunnel vrf fvrf-hub
 tunnel protection ipsec profile DMVPN-PROFILE
 ip virtual-reassembly
```

Configure Enterprise and IDMZ-Connected Interfaces

The DMVPN hub router is connected to a single Enterprise firewall as well as two IDMZ firewalls. A port channel was created to connect from the single DMVPN hub router to the two firewalls. Table 3-2 shows the interfaces and IP addresses used in this CVD.

Table 3-2 DMVPN Hub Router #1 Enterprise and IDMZ-Connected Interfaces and IP Addresses

ASR-HUB1 Interface	Interface	IP address
Connected to Enterprise Firewall	Gi0/0/0	172.24.1.4
Connected to IDMZ Firewall-1	Port Channel 6.600 (Gi0/0/4)	172.25.1.5
Connected to IDMZ Firewall-2	Port Channel 6.600 (Gi0/0/1)	172.25.1.5

Enter global configuration mode and enter the following configuration:

```
!
interface Port-channel6
 description to IDMZ
```

```
 no ip address
 negotiation auto
!
interface Port-channel6.600
 encapsulation dot1Q 600
 ip address 172.25.1.5 255.255.255.0
!
interface GigabitEthernet0/0/0
 description To VPN-DMZ towards Internet
 ip vrf forwarding fvrf-hub
 ip address 172.24.1.4 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 channel-group 6 mode active
!
interface GigabitEthernet0/0/4
 no ip address
 negotiation auto
 channel-group 6 mode active
```

Configure Enhanced Interior Gateway Routing Protocol

EIGRP is a network protocol that allows routers to exchange routing information. This CVD used EIGRP to pass route information between the main site Industrial WAN zone, the remote site(s), and the main site Industrial Zone.

```
router eigrp 101
 network 14.14.14.1 0.0.0.0
 network 172.24.1.0 0.0.0.255
 network 172.25.1.0 0.0.0.255
```

Add a Route to the Enterprise Firewall

In this example, the Enterprise firewall interface that is connected to the DMVPN hub is set to 172.24.1.1. A static route to the Enterprise firewall must be added to the DMVPN router.

Enter global configuration mode and enter the following configuration.

```
ip route vrf fvrf-hub 0.0.0.0 0.0.0.0 172.24.1.1
```

Configuring the Enterprise Firewall

For adding the Enterprise Firewall rules, the configuration has the following major steps:

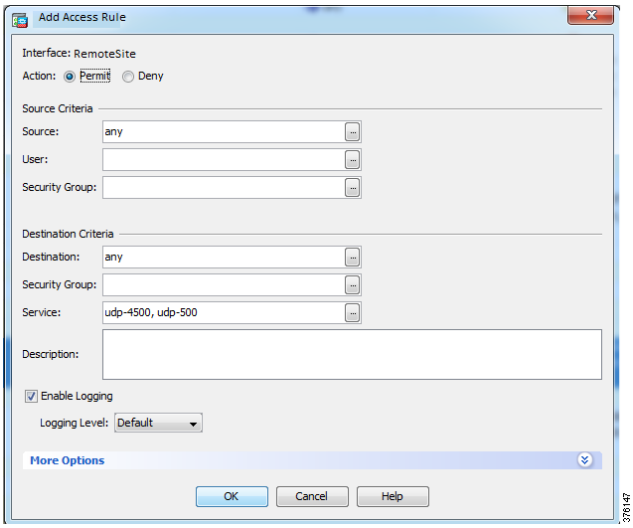
1. Permit Security Associations and Key Exchanges
2. Create Network Object to Represent the DMVPN Hub Router
3. Create NAT Rule

Permit Security Associations and Key Exchanges

The Enterprise firewall must be configured to allow ISAKMP, UDP port 500, and IPsec NAT-T, UDP port 4500 traffic from the interface that connects to the Internet. The tunnel instantiation traffic will be initiated from the remote site spoke routers to the Enterprise firewall.

Using Adaptive Security Device Manager (ASDM), select **Configuration > Firewall > Access Rules**. Select the interface that is connected to the remote site and add the following configuration. In this guide, the firewall interface that is used to connect to the remote site spoke routers is named *RemoteSite*. See Figure 3-1 below.

Figure 3-1 Configuring the Enterprise Firewall Add Access Rule



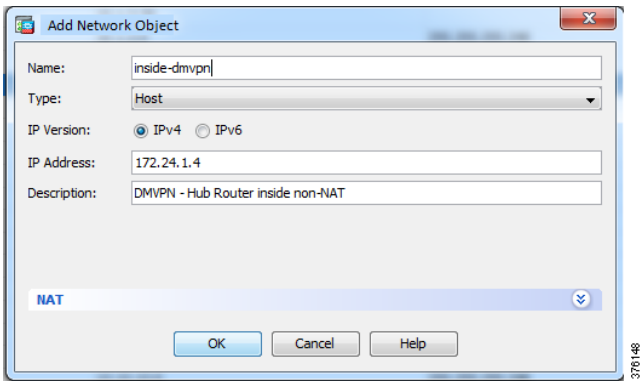
Click **OK** and then click **Apply**.

Create Network Object to Represent the DMVPN Hub Router

Create a network object to define the DMVPN hub router's IP address.

Using ASDM, select **Configuration -> Firewall -> Objects -> Network Objects**. Click **Add > Network Object** and enter the following configuration. See Figure 3-2 below.

Figure 3-2 Configuring the Enterprise Firewall Add Network Object



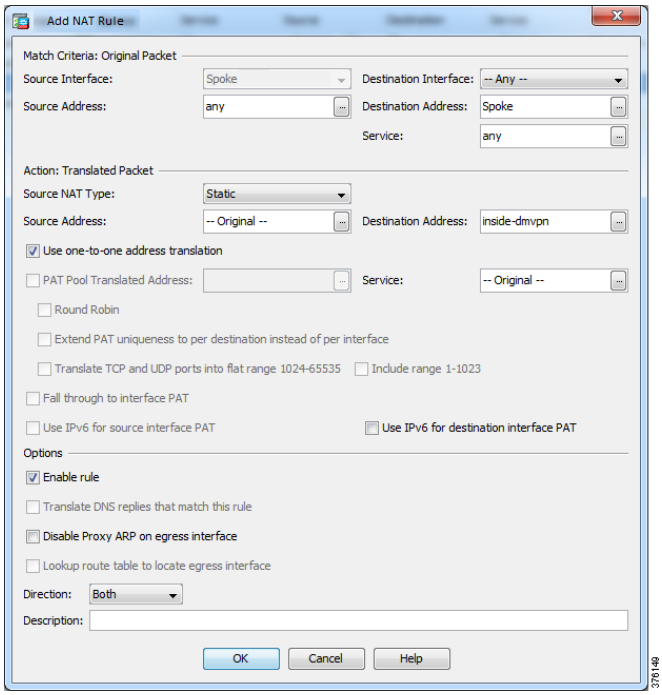
Click **OK** and then click **Apply**.

Create NAT Rule

Configure a 1:1 NAT rule from the firewall interface that will receive remote site spoke traffic. In our example, the source interface is named *Spoke*. The destination IP address for the NAT translation is the ASR router IP address that was defined by the network object *inside-dmvpn*.

Using ASDM, select **Configuration > Firewall > NAT Rules**. Click **Add** and then enter the following configuration. See Figure 3-3 below.

Figure 3-3 Configuring the Enterprise Firewall Add MAT Rule



Click **OK** and then click **Apply**.

Configuring the IDMZ Firewall

For this CVD, we will use the existing IDMZ firewall and configure a new interface to connect to the DMVPN hub router. The IDMZ firewall was already configured as per the CPwE Securely Traversing IACS Data across the Industrial Demilitarized Zone with the interfaces and security levels shown in Table 3-3.

Table 3-3 Configuring the IDMZ Firewall Interfaces and Security Levels

Interface	Security Level	Configured in IDMZ Design Guide / New configuration for this Design Guide
Enterprise	0	IDMZ
IDMZ	75	IDMZ
Industrial	100	IDMZ

By default, a firewall will pass traffic from a higher security level to a lower security level without configuring additional firewall rules. Because of this firewall default behavior, we will explicitly add *permit* rules allowing the Remote Access Server (RAS), which has RSLinx and Studio 5000 software to communicate with the two remote site ControlLogix processors. Explicit *deny* rules will be added to deny CIP communications to any other destinations.

For adding the IDMZ Firewall rules, the configuration has the following major steps:

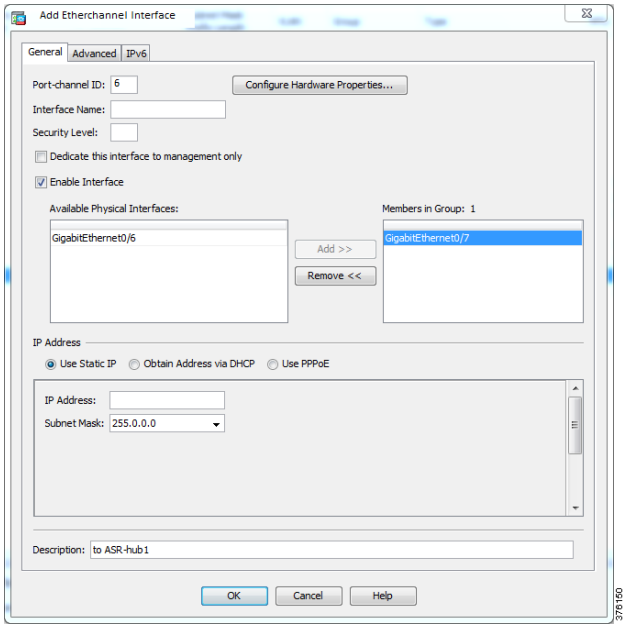
1. Configuring EtherChannel Interface
2. Assigning EtherChannel (Port-Channel) IP Address
3. Creating Remote Site Network Object group
4. Creating Service Group
5. Explicit permit of Remote Access Server (RAS) communication to remote site controllers
6. Explicit deny of Remote Access Server (RAS) communication
7. Ordering of the firewall access rules
8. Allowing Remote Desktop protocol
9. Allowing Messages from Main Site Controller to Remote Site Controller

Configure EtherChannel Interface

The IDMZ firewall in this CVD were implemented as a pair for resiliency. The IDMZ firewall connects to the DMVPN router via EtherChannel. GigabitEthernet 0/7 is the physical interface used in this guide.

Using ASDM, select **Configuration > Device Setup > Interfaces**. Click **Add Etherchannel Interface** and enter the following configuration. See Figure 3-4.

Figure 3-4 Configuring the IDMZ Firewall Add Etherchannel Interface



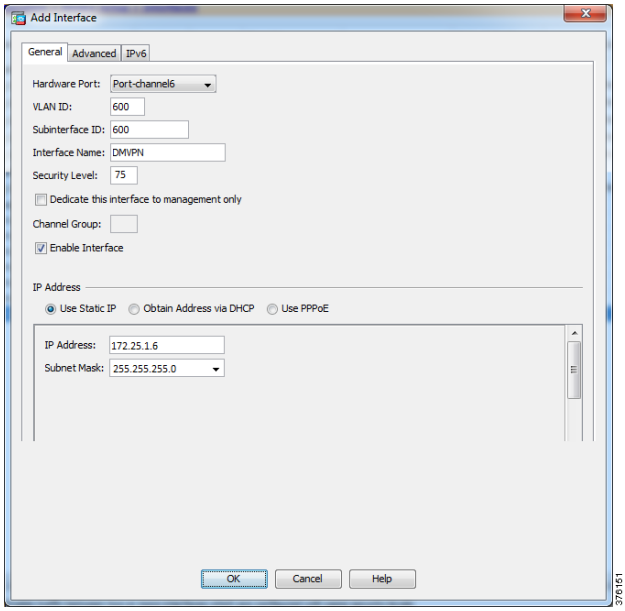
Click **OK** and then click **Apply**.

Assign Etherchannel (Port-Channel) IP address

In the previous step, an EtherChannel was created. In this step, the IP address is assigned to Port-channel.

Using ASDM, select **Configuration > Device Setup > Interfaces**. Click **Add Interface** and enter the following configuration. See Figure 3-5.

Figure 3-5 Configuring the IDMZ Firewall Add Interface



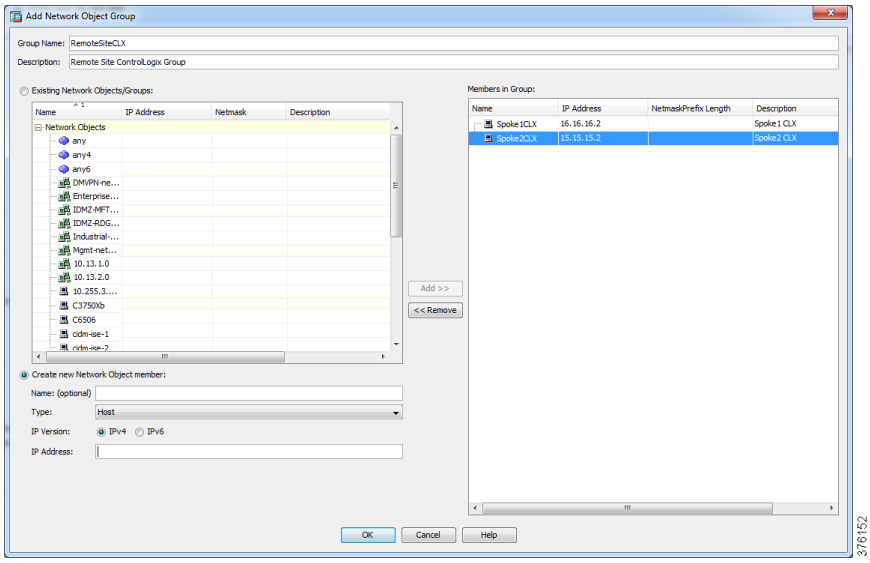
Click **OK** and then click **Apply**.

Create Remote Site Network Object Group

Create the network objects for the ControlLogix controllers at each remote site. This will help simplify the firewall rules by simply using grouping. Controllers can be added or removed without changing the firewall access rules.

Using ASDM, select **Configuration > Firewall > Objects > Network Object Groups**. Click **Add** and then enter the following configuration. See Figure 3-6.

Figure 3-6 Configuring the IDMZ Firewall Add Network Object Group



Click **OK** and then click **Apply**.

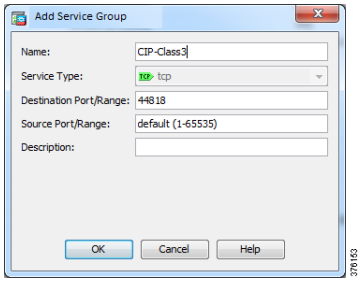
Create a service object for the CIP Class 3 protocol that is used by RSLinx to communicate with the controllers at each remote site.

Create Service Group

By defining protocols as a service group, this protocol can be easily used within a firewall access rule and make the rules more easily understood. By adding CIP-Class3 to this list, we can more easily understand a firewall rule that is used for permitting and denying this IACS control protocol.

Using ASDM, select **Configuration > Firewall > Objects > Service Object**. Click **Add** and then enter the following configuration. See Figure 3-7.

Figure 3-7 Configuring the IDMZ Firewall Add Service Group



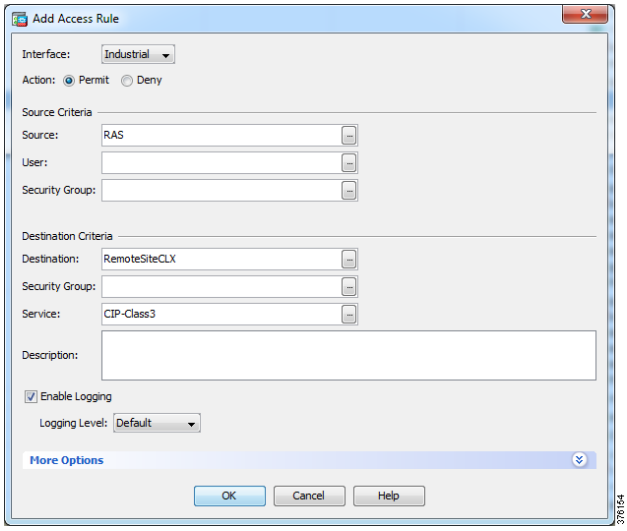
Click **OK** and then click **Apply**.

Explicit Permit of RAS Communication to Remote Site Controllers

Add the explicit permit rule to allow the RAS to communicate with the remote site ControlLogix processor. In the figure below, the RAS source is the IP address of your RAS or engineering workstation.

Using ASDM, select **Configuration > Firewall > Access Rules**. Click **Add** and then enter the following configuration. See Figure 3-8.

Figure 3-8 Configuring the IDMZ Firewall Add Access Rule



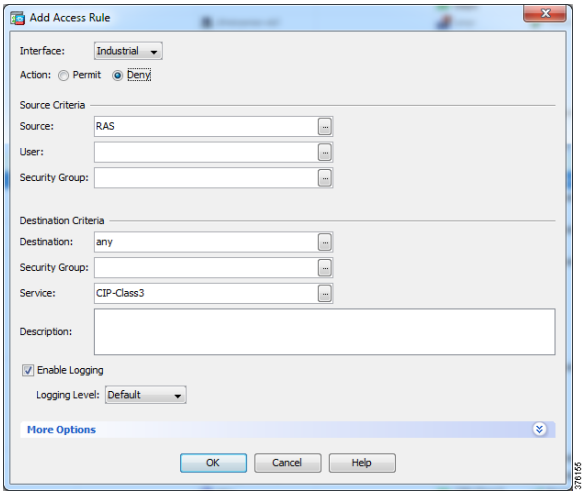
Click **OK** and then click **Apply**.

Explicit Deny of RAS Communication

Add the explicit deny rule to block the RAS from communicating via the CIP protocol to all other locations. In the figure below, the RAS source is the IP address of your RAS or engineering workstation.

Using ASDM, select **Configuration > Firewall > Access Rules**. Click **Add** and then enter the following configuration. See Figure 3-9.

Figure 3-9 Configuring the IDMZ Firewall Add Access Rule

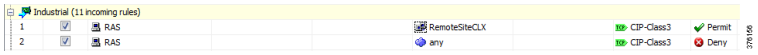


Click **OK** and then click **Apply**.

Ordering of the Firewall Access Rules

The order of the access control rules is important as they are solved from top to bottom. Make sure the permit rule is before the deny rule. See Figure 3-10.

Figure 3-10 Configuring the IDMZ Firewall Ordering of Firewall Access Rules

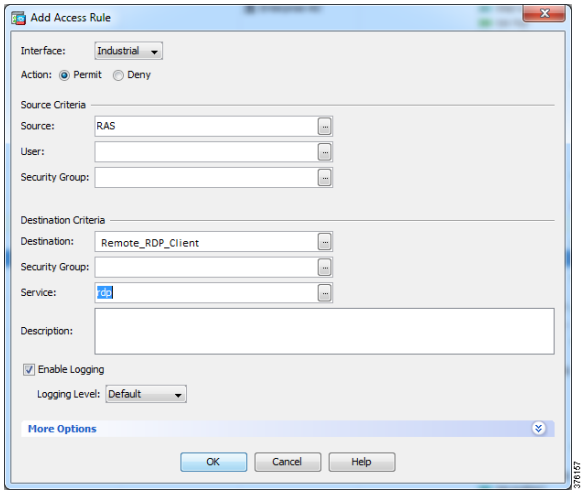


If a rule needs to be moved up or down in the order, this can be done by using ASDM, select **Configuration > Firewall > Access Rules** and then click the up or down arrow. Click **Apply**.

Allowing Remote Desktop Protocol

If Remote Desktop Protocol is required to access a desktop at the remote site from the RAS then this protocol should be explicitly permitted by configuring the firewall rules. Using ASDM, select **Configuration > Firewall > Access Rules**. Click **Add** and then enter the following configuration. See Figure 3-11.

Figure 3-11 Configuring the IDMZ Firewall Add Access Rule



Click **OK** and then click **Apply**.

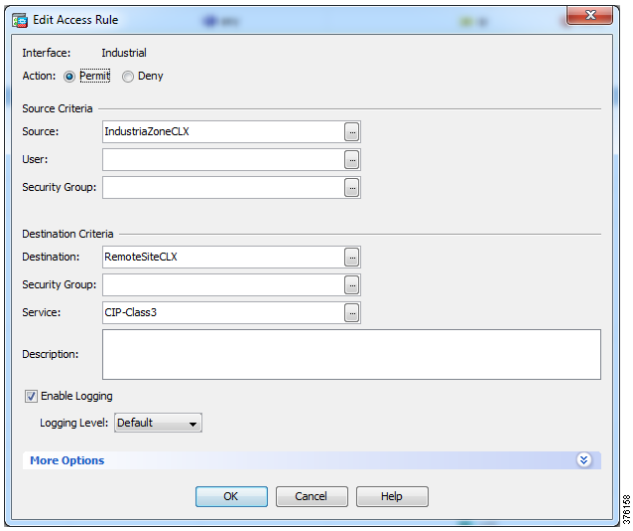
Note Configure an explicit deny rule that denies all traffic from the RAS to other destinations.

Allowing Messages from Main Site Controller to Remote Site Controller

If a message instruction is used to pass data between a main site controller and a remote site controller, a CIP-Class3 (port 44818) firewall rule permitting the traffic is required. In this guide, the main site controller source is named *IndustrialZoneCLX*. The remote site controller(s) are named *RemoteSiteCLX*.

Using ASDM, select **Configuration > Firewall > Access Rules**. Click **Add** and then enter the following configuration. See Figure 3-12.

Figure 3-12 Configuring the IDMZ Firewall Add Access Rule



Click **OK** and then click **Apply**.

Note Configure an explicit deny rule that denies all traffic from the RAS to other destinations.

Configuring Remote-Site DMVPN Spoke Router #1

This configuration has the following major steps:

1. Configuring the Router Host Name
2. Setting the Clock Time Zone
3. Creating the Front door VRF
4. Creating the Inside VRF
5. Creating the Internet Security Association and Key Management Protocol for IPsec
6. Configuring the GRE tunnel Interface
7. Creating a Loopback Interface to Support NAT
8. Configuring a Static 1:1 NAT
9. Creating the VLAN
10. Configuring the WAN Interface
11. Configuring Enhanced Interior Gateway Routing Protocol
12. Adding a Route to Main Site Enterprise Firewall
13. Setting the NTP Server

Configure the Router Host Name

Enter global configuration mode and enter the remote site router #1's host name.

```
hostname spoke1
```

Set the Clock Time Zone

Set the clock time zone by entering the following commands. Your configuration may vary based on your location and time zone.

```
clock timezone EST -5 0
clock summer-time EDT recurring
```

Create the Front Door VRF

An Internet-facing VRF is created to support FVRF for DMVPN. The FVRF name for the spoke router in this CVD is *fvrf-spoke1*. An associated RD must also be configured to make the FVRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the FVRF instance.

This design uses VRF Lite so that the RD value can be chosen arbitrarily but it is a recommended best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

The RD for this FVRF is 5:5.

```
vrf definition fvrf-spoke1
 rd 5:5
 !
 address-family ipv4
  route-target export 5:5
  route-target import 5:5
 exit-address-family
```

Create Inside VRF

In this configuration, the spoke 1 inside VRF is named *ivrf-spoke1* and the RD for this VRF is 6:6.

```
vrf definition ivrf-spoke1
 rd 6:6
 !
 address-family ipv4
  route-target export 6:6
  route-target import 6:6
 exit-address-family
```

Create the Internet Security Association and Key Management Protocol for IPsec

ISAKMP policies can be configured for authentication from PSKs or digital certificates. This CVD used PSKs for Stratix 5900 remote site spoke router due to limitations of certificate support. If certificate support is required, it is recommended that a suitable Cisco platform is used as the remote site spoke router.

Step 1 Configure the crypto keyring.

The crypto keyring defines a PSK (or password) valid for IP sources that are reachable within a particular VRF. This key is a wildcard PSK if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING1 vrf fvrf-spoke1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 2 Configure the ISAKMP policy.

The ISAKMP policy for DMVPN uses the following:

- AES with a 256-bit key
- SHA
- Authentication by PSK
- Diffie-Hellman group: 2

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp keepalive 30 5
```

Step 3 Create the ISAKMP Profile.

The ISAKMP profile creates an association between an identity address, a VRF, and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 fvrf-spoke1
```

Step 4 Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for this DMVPN example uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
```

Step 5 Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
```

Step 6 Increase the IPsec anti-replay window size.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed. It is recommended that the maximum window size be used to minimize future anti-replay problems. On the Stratix 5900, the maximum replay window size was set to 1024.

If the window size is not increased, the router may drop packets and the following error message may display on the router CLI:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
crypto ipsec security-association replay window-size 1024
```

Configure the GRE Tunnel Interface

The remote site spoke routers will connect to the main site DMVPN hub router via the GRE tunnel interface. For this CVD, the parameters shown in Table 3-4 are used.

Table 3-4 Configure the GRE Tunnel Interface Parameters

Device Host Name	Tunnel 0 IP address	EIGRP AS	NHRP Map	NHRP Network ID
Spoke1	14.14.14.5 /24	101	14.14.14.1 mapped to 11.11.11.1	101

Enter global configuration mode and enter the following configuration for GRE Tunnel 0.

```
interface Tunnel0
 ip address 14.14.14.5 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 101 35
 no ip next-hop-self eigrp 101
 no ip split-horizon eigrp 101
 ip pim dr-priority 0
 ip pim sparse-mode
 ip nat outside
 ip nhrp authentication cisco123
 ip nhrp map multicast 11.11.11.1
 ip nhrp map 14.14.14.1 11.11.11.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 14.14.14.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip virtual-reassembly in
 tunnel source GigabitEthernet0
 tunnel mode gre multipoint
 tunnel vrf fvrf-spoke1
 tunnel protection ipsec profile DMVPN-PROFILE1
```

Create a Loopback Interface to Support NAT

A loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, a loopback address was assigned to an address within the public NAT network IP address range. In our example, the public NAT IP address is 16.16.16.2 / 24 so the loopback address 16.16.16.1 is within the same network. Enter the following configuration:

```
interface Loopback16
 ip address 16.16.16.1 255.255.255.0
```

Configure a Static 1:1 NAT

In this example, a 1:1 NAT is configured to allow the ControlLogix IP address configuration to remain statically assigned. In this example, the ControlLogix private IP address is set to 192.168.1.102. The outside public address for this ControlLogix controller is 16.16.16.2. Enter global configuration mode and enter the following configuration:

```
ip nat inside source static 192.168.1.102 16.16.16.2
```

Create VLAN 10

In this example, the access ports on the Stratix 5900 are set to VLAN 10 and the ControlLogix controller is directly connected to the Stratix 5900. Enter global configuration mode and enter the following configuration:

```
interface Vlan10
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in

interface FastEthernet0
 switchport access vlan 10
 no ip address
!
interface FastEthernet1
 switchport access vlan 10
 no ip address
!
interface FastEthernet2
 switchport access vlan 10
 no ip address
!
interface FastEthernet3
 switchport access vlan 10
 no ip address
!
```

Configure the WAN Interface

The WAN interface, GigabitEthernet (GE) 0, is used as the source for the front door VRF. In this guide, the IP address was statically set to 11.11.11.2 /24. A simple access list was added to deny all traffic except for tunnel traffic into the WAN interface. Enter global configuration mode and enter the following configuration.

```
interface GigabitEthernet0
 vrf forwarding fvrf-spoke1
 ip address 11.11.11.2 255.255.255.248
 ip access-group 101 in
 ip virtual-reassembly in
 duplex auto
 speed auto
!
! permit tunnel creation
access-list 101 permit udp 11.11.11.1 0.0.0.0 any eq 500
access-list 101 permit udp 11.11.11.1 0.0.0.0 any eq 4500
access-list 101 deny tcp any any
```

Configure Enhanced Interior Gateway Routing Protocol

EIGRP is a network protocol that allows routers to exchange routing information. This CVD used EIGRP to pass route information between the main site Industrial WAN zone, the remote site(s), and the main site Industrial Zone. Enter global configuration mode and enter the following configuration.

```
router eigrp 101
 network 14.14.14.5 0.0.0.0
 network 16.16.16.0 0.0.0.255
```

Add a Route to Main Site Enterprise Firewall

In this example, the Enterprise firewall connects to the Internet and is statically configured for 11.11.11.1. A default static route to the Enterprise firewall must be added to the remote site spoke routers.

Enter global configuration mode and enter the following configuration.

```
ip route vrf fvrf-spoke1 0.0.0.0 0.0.0.0 11.11.11.1
```

Set NTP Server

Set the IP address of the company's NTP Server.

```
ntp server xxx.xxx.xxx.xxx
```

Note In the above example, substitute *xxx.xxx.xxx.xxx* with your company's NTP server IP address.

Configuring Remote-Site DMVPN Spoke Router (Router 2)

This configuration has the following major steps:

1. Configuring the Router Host Name
2. Setting the Clock Time Zone
3. Creating the Front door VRF
4. Creating the Inside VRF
5. Creating the Internet Security Association and Key Management Protocol for IPsec
6. Configuring the GRE Tunnel Interface
7. Creating a Loopback Interface to Support NAT
8. Configuring a Static 1:1 NAT
9. Creating the VLAN
10. Configuring the WAN Interface
11. Configuring Enhanced Interior Gateway Routing Protocol
12. Adding a Route to Main Site Enterprise Firewall
13. Setting the NTP Server

Configure the Router Host Name

Enter global configuration mode and enter the remote site router #2's host name.

```
hostname spoke2
! Set the clock time zone
```

Set the clock time zone by entering the following commands. The configuration may vary based on location and time zone.

```
clock timezone EST -5 0
clock summer-time EDT recurring
```

Create the Front Door VRF

An Internet-facing VRF is created to support FVRF for DMVPN. The FVRF name for the spoke router in this CVD is *fvrf-spoke2*. An associated RD must also be configured to make the FVRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the FVRF instance. This design uses VRF Lite so that the RD value can be chosen arbitrarily, but it is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

The RD for this FVRF is 4:4.

```
vrf definition fvrf-spoke2
 rd 4:4
 !
 address-family ipv4
  route-target export 4:4
  route-target import 4:4
 exit-address-family
```

Create Inside VRF

In this configuration, the spoke 2 inside VRF is named *ivrf-spoke2* and the RD for this VRF is 3:3.

```
vrf definition ivrf-spoke2
 rd 3:3
 !
 address-family ipv4
  route-target export 3:3
  route-target import 3:3
 exit-address-family
```

Create the ISAKMP for IPsec

ISAKMP policies can be configured for authentication from PSKs or digital certificates. This CVD used PSKs for Stratix 5900 remote site spoke router due to certificate support limitations. If certificate support is required, it is recommended that a suitable Cisco platform is used as the remote site spoke router.

Step 1 Configure the crypto keyring.

The crypto keyring defines a PSK (or password) valid for IP sources that are reachable within a particular VRF. This key is a wildcard PSK if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING1 vrf fvrf-spoke2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 2 Configure the ISAKMP policy.

The ISAKMP policy for DMVPN uses the following:

- AES with a 256-bit key
- SHA
- Authentication by PSK
- Diffie-Hellman group: 2

```
crypto isakmp policy 10
```

```
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp keepalive 30 5
```

Step 3 Create the ISAKMP Profile.

The ISAKMP profile creates an association between an identity address, a VRF, and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 fvrf-spoke2
```

Step 4 Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for this DMVPN example uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
```

Step 5 Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
```

Step 6 Increase the IPsec anti-replay window size.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed. It is recommended that the maximum window size be used to minimize future anti-replay problems. On the Stratix 5900, the maximum replay window size was set to 1024. If the window size is not increased, the router may drop packets and the following error message may appear on the router CLI:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
crypto ipsec security-association replay window-size 1024
```

Configure the GRE Tunnel Interface

The remote site spoke routers will connect to the main site DMVPN hub router via the GRE tunnel interface. For this CVD, the parameters shown in Table 3-5 are used:

Table 3-5 Configure the GRE Tunnel Interface Parameters

Device Host Name	Tunnel 0 IP address	EIGRP AS	NHRP Map	NHRP Network ID
Spoke2	14.14.14.6 /24	101	14.14.14.1 mapped to 11.11.11.1	101

Enter global configuration mode and enter the following configuration for GRE Tunnel 0.

```
interface Tunnel0
 ip address 14.14.14.6 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hold-time eigrp 101 35
 no ip next-hop-self eigrp 101
 no ip split-horizon eigrp 101
 ip pim dr-priority 0
 ip pim sparse-mode
 ip nat outside
 ip nhrp authentication cisco123
 ip nhrp map multicast 11.11.11.1
 ip nhrp map 14.14.14.1 11.11.11.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 14.14.14.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip virtual-reassembly in
 tunnel source GigabitEthernet0
 tunnel mode gre multipoint
 tunnel vrf fvrf-spoke2
 tunnel protection ipsec profile DMVPN-PROFILE1
```

Create a Loopback Interface to Support NAT

A loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, a loopback address was assigned to an address within the public NAT network IP address range. In our example, the public NAT IP address is 16.16.16.2 / 24 so the loopback address 16.16.16.1 is within the same network. Enter global configuration mode and enter the following configuration.

```
interface Loopback15
 ip address 15.15.15.1 255.255.255.0
```

Configure a Static 1:1 NAT

In this example, a 1:1 NAT is configured to allow the ControlLogix IP address configuration to remain statically assigned. In this example, the ControlLogix private IP address is set to 192.168.1.102. The outside public address for this ControlLogix controller is 16.16.16.2. Enter global configuration mode and enter the following configuration.

```
ip nat inside source static 192.168.1.102 15.15.15.2
```

Create VLAN 10

In this example, the access ports on the Stratix 5900 are set to VLAN 10 and the ControlLogix controller is directly connected to the Stratix 5900. Enter global configuration mode and enter the following configuration.

```
interface Vlan10
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in

interface FastEthernet0
 switchport access vlan 10
```

```
 no ip address
!
interface FastEthernet1
 switchport access vlan 10
 no ip address
!
interface FastEthernet2
 switchport access vlan 10
 no ip address
!
interface FastEthernet3
 switchport access vlan 10
 no ip address
!
```

Configure the WAN Interface

The WAN interface, GigabitEthernet 0, is used as the source for the front door VRF. Enter global configuration mode and enter the following configuration.

```
interface GigabitEthernet0
 vrf forwarding fvrf-spoke1
 ip address 11.11.11.3 255.255.255.248
 ip virtual-reassembly in
 duplex auto
 speed auto
```

Configure Enhanced Interior Gateway Routing Protocol

EIGRP is a network protocol that allows routers to exchange routing information. This CVD used EIGRP to pass route information between the main site Industrial WAN zone, the remote site(s), and the main site Industrial Zone. Enter global configuration mode and enter the following configuration.

```
router eigrp 101
 network 14.14.14.6 0.0.0.0
 network 15.15.15.0 0.0.0.255
```

Add a Route to Main Site Enterprise Firewall

In this example, the Enterprise firewall connects to the internet and is statically configured for 11.11.11.1. A default static route to the Enterprise firewall must be added to the remote site spoke routers. Enter global configuration mode and enter the following configuration.

```
ip route vrf fvrf-spoke1 0.0.0.0 0.0.0.0 11.11.11.1
```

Set NTP Server

Set the IP address of the company's NTP Server.

```
ntp server xxx.xxx.xxx.xxx
```

Note In the above example, substitute *xxx.xxx.xxx.xxx* with your company's NTP server IP address.

APPENDIX A

References

The following references are relevant to what is discussed in this DIG.

- *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide:*
  - Rockwell Automation site:
    - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site:
    - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html
- *Deploying the Resilient Ethernet Protocol (REP) in a Converged Plantwide Ethernet System (CPwE) Design Guide:*
  - Rockwell Automation site:
    - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td005_-en-p.pdf
  - Cisco site:
    - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/REP/CPwE_REP_DG.html
- *Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:*
  - Rockwell Automation site:
    - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
  - Cisco site:
    - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- *Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:*
  - Rockwell Automation site:
    - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
  - Cisco site:

  - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

- *Deploying Identity Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide*:
  - Rockwell Automation site:
    - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
  - Cisco site:
    - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html
- *Securely Traversing Industrial Automation Control System (IACS) Data Across the Industrial Demilitarized Zone Design and Implementation Guide*:
  - Rockwell Automation Site:
    - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco Site:
    - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/WP/CPwE_IMDZ_WP/CPwE_IMDZ.html
- *Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide*:
  - Rockwell Automation Site:
    - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
  - Cisco Site:
    - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/4-0/Resiliency/DIG/CPwE_resil_CVD.html
- *Cisco VPN WAN Technology Design Guide*:
  - http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-VPNWANDesignGuide-AUG14.pdf
- *Dynamic Multipoint VPN*:
  - http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-2mt/sec-conn-dmvpn-dmvpn.html#GUID-D8F6839F-D735-4C8E-A199-602CDD8F7DD0

APPENDIX B

Test Hardware and Software

Table B-1 lists test hardware and software used in this CVD.

Table B-1 Test Hardware and Software

Role	Product	SW Version	Notes
Main Site DMVPN Router	Cisco ASR1004 (RP2) Processor (revision RP2)	ASR1000 Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(2)S2,	
Remote Site 1 and 2 Router	Stratix 5900	15.3(3)M	
Rockwell Automation Software®	RSLinx® Classic	3.73.00	
Rockwell Automation Software	Studio 5000® Logix Designer	26.01	
Programmable Automation Controller	1756 ControlLogix Controller	26.012	1756-L75/B,
EtherNet/IP Communication Module	ControlLogix 2-port EtherNet/IP Module	4.004 5.028	1756-EN2TR

APPENDIX C

Acronyms and Initialisms

Table C-1 lists acronyms and initialisms used in this document.

Table C-1 Acronyms and Initialisms

Term	Definition
1:1	One-to-One
AES	Advanced Encryption Standard
AH	Authentication Header
ASDM	Cisco Adaptive Security Device Manager
ASR	Cisco Aggregation Services Router
CIP	Common Industrial Protocol
CPwE	Converged Plantwide Ethernet
CVD	Cisco Validated Design
DIG	Design and Implementation Guide
DMVPN	Dynamic Multipoint Virtual Private Network
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Protocol
FIB	Forwarding Information Base
FVRF	Front-door Virtual Route Forwarding
GRE	Generic Routing Encapsulation
HMAC	Hash Message Authentication Code
IACS	Industrial Automation and Control System
IDMZ	Industrial Demilitarized Zones
IKE	Internet Key Exchange
IP	Internet Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ISR	Integrated Service Router
mGRE	Multipoint Generic Routing Encapsulation
MPLS	Multiprotocol Label Switching
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAT	Network Address Translation

Table C-1 Acronyms and Initialisms (continued)

Term	Definition
NHRP	Next Hop Routing Protocol
PAT	Port Address Translation
PSK	Pre-Shared Key
RAS	Remote Access Server
RD	Route Descriptor
SA	Security Association
SHA	Secure Hash Standard
SYN	Synchronization
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
WAN	Wide Area Network
ZFW	Zone-Based Policy Firewall

Publication ENET-TD012A-EN-P March 2016