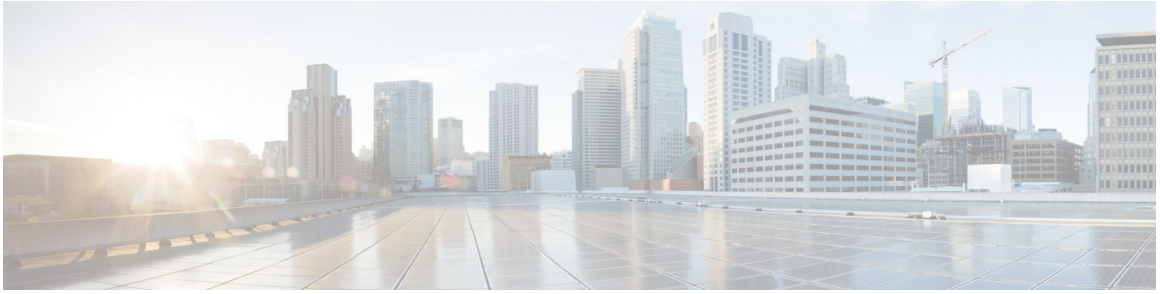
Control Center Virtualization for the Connected Pipeline System Implementation Guide

May 2016

Control Center Virtualization for the Connected Pipeline Implementation Guide



Preface

Oil and Gas Pipeline management is challenging, with pipelines often running over large geographical distances, through harsh environments, and with limited communications and power infrastructure available. In addition, pipelines must comply with stringent environmental regulations and operate as safely as possible, as well as addressing growing cyber and physical security threats.

Critical pipelines requirements, however, have not changed. Pipeline availability, integrity, safety, security, and reliability are essential elements that help operators meet demanding delivery schedules and optimize operational costs.

Validated designs make deploying host Pipeline Management System (PMS) environments easier. Validated designs describe solutions using various equipment types and technologies that are designed, tested, and documented, to facilitate, simplify, and improve customer deployments and address their business needs.

An integrated design delivers on the promise of maximum reliability with a single cohesive system that integrates Supervisory Control and Data Acquisition (SCADA) services and operational applications, network traffic, embedded management, and powerful servers with high-speed hard disks and memory. Integrated design provides performance through a better architecture and better balance of resources that:

- Simplifies physical and virtual networks, reducing cost while increasing manageability
- Scales better and more rapidly and with lower infrastructure cost per server
- Delivers greater flexibility with virtualized environments for development and testing
- Increases an organization's responsiveness to changing workloads and business conditions through increased flexibility

With a jointly architected and validated approach to Pipeline management, networking, and computing realizable benefits can be significant. Solution integration quality and interoperability are maximized, while design and testing time are minimized. End users have a single point of reference accountable for integration and operational success from hardware, software, security, and management perspectives throughout the lifecycle of a project. The jointly architected design will provide maximum benefit for current operations and be a platform for future application enablement and integration.

This *Control Center Virtualization for the Connected Pipeline System Implementation Guide* documents best practice design and implementation of safe, highly available, and secure infrastructure and applications for Oil and Gas Pipelines. The purpose of this document is to identify customer use cases, map those use cases to relevant architectures, and leverage Cisco and partner technology to deliver unprecedented value for our customers. This document:

  - Describes a Low Level Design (LLD) detailing Control Center Virtualization for the Connected Pipeline System. It will provide guidance supporting SCADA principles, unified networking and powerful compute for the Control Center.

- Documents best practices from real world implementations, detailing the designs and architectures that are mapped back to the customer use cases.
- Addresses real-life customer deployment scenarios by providing a solution that supports implementation of a scalable, secure, and redundant operational network supporting both industrial and multi-service applications.
- Details support for implementing Control Center application virtualization, secure remote access, the Industrial Demilitarized Zone (IDMZ), and cyber security.
- Specifies topology, QoS, high availability, security services, network management services, and Control Center virtualization implementations.
- Provides information about enforcing cyber security best practices that follow the recognized Industrial Control System (ICS) security standards and guidelines including ISA99/IEC 62443, the NIST Cyber Security Framework, and the Purdue Model of Control.
- Documents the suggested equipment and technologies, system level configurations, and recommendations. It also includes description of caveats and considerations that Pipeline operators should understand as they implement best practices.
- Although this CVD focuses on midstream transport Pipelines, the technologies, use cases, and principles are applicable for gathering and distribution Pipelines.

Document Objective and Scope

In this initial release, Cisco has partnered with Schneider Electric to provide architecture, design, and technologies for the Control Centers, Operational telecoms network, and the pipeline stations. Cisco provides infrastructure expertise with its unified compute and networking security platforms while Schneider Electric provides the PMS (PMS) leadership with its OASyS Dynamic Network of Applications (DNA) SCADA system hardware and software.

The release will focus on the Control Center environment and security architecture to support pipeline operators. It is recommended that the reader become familiar with the following joint Cisco/Schneider Electric white papers:

- *Integrated Enterprise SCADA System Architectures for Safe and Efficient Pipeline Operations* at the following URL:
  - http://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/dlfe-683318406.pdf
- *Converged Telecommunication Architectures for Effective Integrated Pipeline Operations* at the following URL:
  - http://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/dlfe-683318407.pdf

As with any architecture and design program, functional requirements, use cases, and architectures evolve. Therefore, this CVD will evolve and will be updated in future phases.

Contributors

The following individuals have contributed to this *Control Center Virtualization for the Connected Pipeline System Implementation Guide*:

- Kiran Ramaswamy, SR. Software Engineer, IoE Vertical Solutions Group, Cisco Systems
- Brandon O'Gorman, Software Engineer, IoE Vertical Solutions Group, Cisco Systems

Implementation Overview

Cisco has designed a unified computing and networking architecture to satisfy the requirements of Control Center virtualization for SCADA applications in the Oil and Gas industry. This effort is in partnership with Schneider Electric and uses their Enterprise Pipeline Management (ePLM) solution. This solution implementation focuses on real-time monitoring and control through sharing and collection of data to a centralized PMS. A PMS combines operational SCADA with real-time applications specific to the Oil and Gas industry, host-based leak detection, and historical flow measurement.

This chapter includes the following topics:

A well-designed PMS uses a hardware and software architecture that allows functions to be mobile, scalable, flexible, and robust. It also permits distribution of processing among different SCADA system components to optimize overall performance of the PMS.

These integrated applications provide Pipeline operators the following:

- Real-time/near real-time control and supervision of operations along the pipeline through a SCADA system based in one or more Control Centers
- Accurate measurement of flow, volume, and levels to ensure correct product accounting
- Ability to detect and locate pipeline leakage including time, volumes, and location distances
- Integrated security systems for personnel, the environment, and infrastructure using video surveillance, access control, and intrusion detection systems
- Ensure safe operations through instrumentation and safety systems
- Energy management system to visualize, manage, and optimize energy consumption within the main stations

The Control Center virtualization solution uses Schneider Electric's OASyS SCADA applications for real-time monitoring and control in a Data Center environment consisting of network, compute, and storage components. The integration of these components forms the basis for the Base Line Integrated SCADA System (BLISS), whose architecture involves a highly redundant framework integrated with security. BLISS comprises multiple zones: Production, Test and Development, and Decision Support System (DSS). This Data Center infrastructure, along with operator stations, can be deployed into any Control Center environment for monitoring and control of Pipeline Operations.

This document is the implementation guide for the Control Center virtualization solution. The salient features of the architecture are the following:

- Cisco Aggregation Services Router (ASR) 902 as Data Center provider edge for connectivity to the wide area MPLS/IP network.
- Pair of ASA 5525-X security appliances providing the redundant firewall capability within the Control Center.
- Use of UCS-B 5108 with B200 M4 blade servers for hosting Schneider's SCADA applications. The blade servers do not have local storage. The SCADA application servers depend on external storage array on EMC VNXe3200 for boot and database purposes.
- Connectivity between the compute, firewall, and edge routers are provided through a pair of FI6248 Fabric Interconnects.
- Cisco Nexus 3524 switches are deployed within the Data Center for segmentation of traffic between the Production, Test and Development, and DSS zones.

Note This implementation involved only one Control Center environment comprising the Production and DSS zones.

Solution Architecture

The Control Center virtualization solution uses a hierarchical network design for redundancy, security, and management. The implementation uses redundant edge routers for connecting the Data Center environment with the Wide Area Network (WAN). Redundant switches for network topology will help ensure failover path for packet forwarding within the Control Center. A pair of redundant firewall appliances help ensure hot/standby setup. VLANs and Virtual Routing and Forwarding (VRF) instances help ensure isolation within the Data Center for different zones. The Control Center virtualization falls into different layers that are briefly explained below:

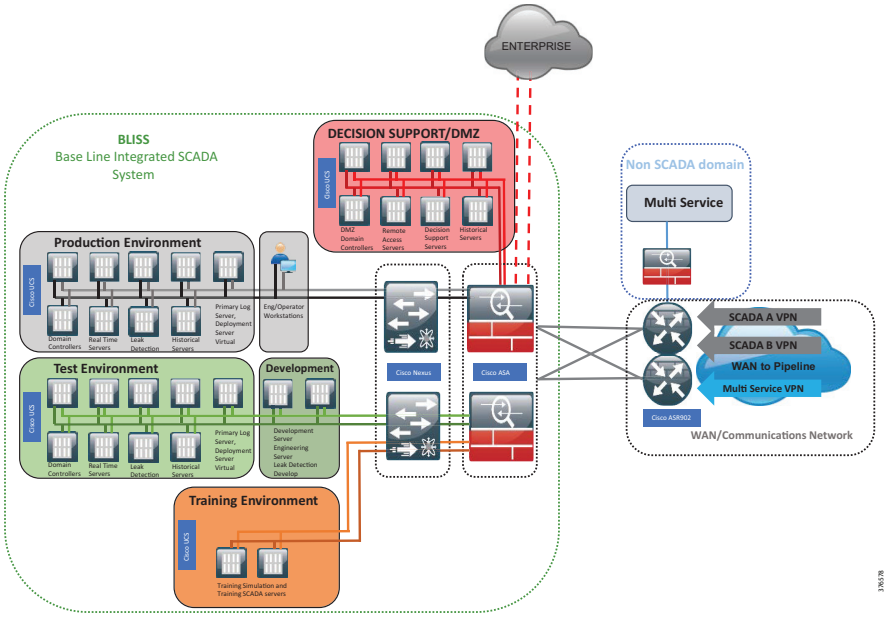
- **Edge/WAN**—The SCADA Control Center will be able to communicate with the pipeline segment via the MPLS/IP-connected WAN. A pair of ASR 902s facilitate communication by providing redundancy for wide area connectivity to the Control Center using Layer 3 Virtual Private Network (L3VPN). Separate routing and forwarding instances in the router provide segmentation of the traffic between different pipeline segments. This pair of routers also provide high availability for connectivity to the Control Center environment.
- **Access**—A pair of Nexus 3524 switches provides connectivity to the server farm in the UCS, Fabric Interconnect, firewalls, and edge routers interfacing with the WAN. Virtual Port Channel (vPC) configurations allow traffic between the connected devices. Appropriate VLANs are configured on the vPCs to ensure segmentation of traffic between pipeline stations and the Production and DSS zones. Operator stations within the Control Center are connected to ports on the same switch. Necessary access VLAN configurations are employed to provide security. Redundant setup of these Nexus switches provide high hardware availability. Unused ports on the switches are placed into shutdown mode. Ports connected to operator stations are configured for port security.
- **Security**—Security within the Control Center is provided by a pair of Adaptive Security Appliances (ASA). ASA 5525 platforms configured in hot/standby mode provide firewall capability within the Control Center. This pair of firewalls also act as the default gateway for all the SCADA application servers within the Control Center (both Production and DSS). All the traffic from the Pipeline traverses the firewall before reaching the SCADA applications and vice versa. Access control policy configured on the firewall determines what traffic is allowed between the Pipeline and Control Center. A set of vPCs between firewall assembly and Nexus switches determines the VLAN segmentation for Production and DSS traffic.

- **Compute**—The SCADA applications in the Production zone are virtualized in a unified computing environment hosted on Cisco Unified Computing System (UCS)-B series servers. Dual redundant UCSB5108 chassis with B200 M4 blades support this infrastructure. SCADA applications hosted in the Production zone include RealTime Service, Domain Controllers, and Historical Service. All of these are hosted as hot/standby-paired applications. The SCADA applications in the DSS zone are virtualized in a unified computing environment hosted on Cisco UCS-C series server. A UCS C220 M4 server is used for this purpose. The SCADA applications hosted in the DSS zone include Domain Controller, RealTime Service, Historical Service, Remote Access, and Reporting Service. Connectivity and access to such a unified computing system are provided through a pair of FI6248 Fabric Interconnect platforms. In addition to connectivity, they also provide hardware redundancy in the Data Center environment.
- **Storage**—Storage for the Historical database is provided on the EMC VNxe3200 platform, connected directly to ports on Fabric Interconnect via fiber channel.

Control Center Overview

The SCADA system provides operators located in a control room the ability to monitor, operate, and control the operations along the Pipeline. The SCADA system consists of multiple environments within the architecture, as outlined in Figure 1-1.

Figure 1-1 Control Center for Oil and Gas



Production Environment

The Production environment enables real-time operations. This consists of RealTime servers, operator Workstations, Historical servers, Logging servers, Leak Detection servers, and any ancillary services such as Domain Controllers. Details about the functionality of such servers can be found in the *Control Center Virtualization for the Connected Pipeline System Design Guide*, which can be found at the following URL:

- https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-11217884

The Production environment servers are hosted on a UCS B200 M4 blade server shared across a dual UCS B5108 chassis framework. The UCS B00M4 servers do not have local storage. The application servers depend on the external storage array EMC VNXe3200 for boot-up and database. A VLAN 120 with an IP address range of 192.168.120.x is used within the Data Center environment for segmentation of the Production zone. The application servers use the firewall setup for the default gateway reaching to the Pipeline Network.

Test and Development

Test and Development systems are a non-Production replica of the operational SCADA system. This environment provide many functions related to source code, initial configurations, code/configuration changes, and maintenance.

Test and Development systems were not implemented as part of the solution.

Decision Support System /Industrial DMZ

The DSS isolates the operational system from any external systems or users. It is updated with real-time and historical data from the live system to provide a secure method of providing real-time data to external users.

The DSS servers are hosted on a UCS C220 M4 rack mount servers with local storage. These servers have adequate local storage and do not rely on the external storage array. A VLAN 125 with an IP address range of 192.168.125.x is used within the Data Center for segmentation of the DSS zone. Policy setup in the firewall helps ensure that no communication will exist between the DSS zone and the Pipeline Network. The only communication servers in DSS zone will be with the Production zone and the Corporate/Enterprise users.

Multi-Service

The multi-service zone in a Control Center is primarily a non-operational environment. It primarily hosts communication services such as physical security and voice and video communication along the Pipeline segment. This multi-service traffic is segregated from the operational SCADA traffic from Pipeline, WAN, and within the Control Center. Cross-pollination of this multi-service traffic will not occur with operational SCADA.

Note The multi-services environment was not implemented as part of the solution.

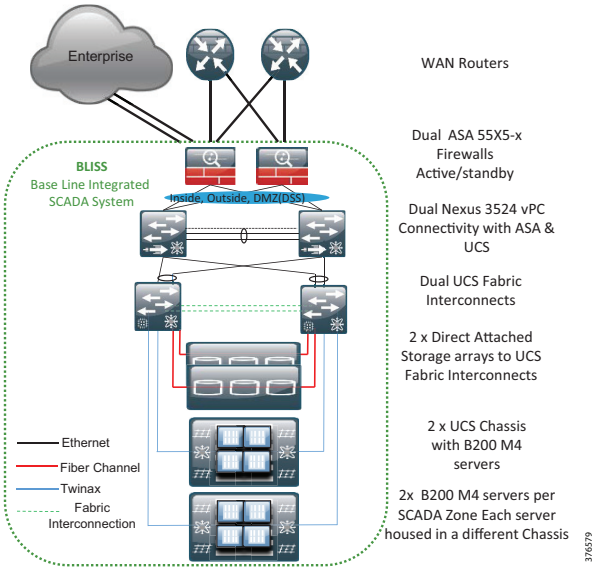
Control Center Availability and Security

This section includes an overview of Control Center availability and security.

Availability

Figure 1-2 shows the high availability design for the Control Center.

Figure 1-2 High Availability Design for Control Center



Design of the BLISS SCADA system mandates redundancy at all applicable levels within the Control Center environment. Refer to Figure 1-2 for redundancy implementation within Control Center environment. High availability is built into compute, network, storage, and application components with the resources made available for the implementation.

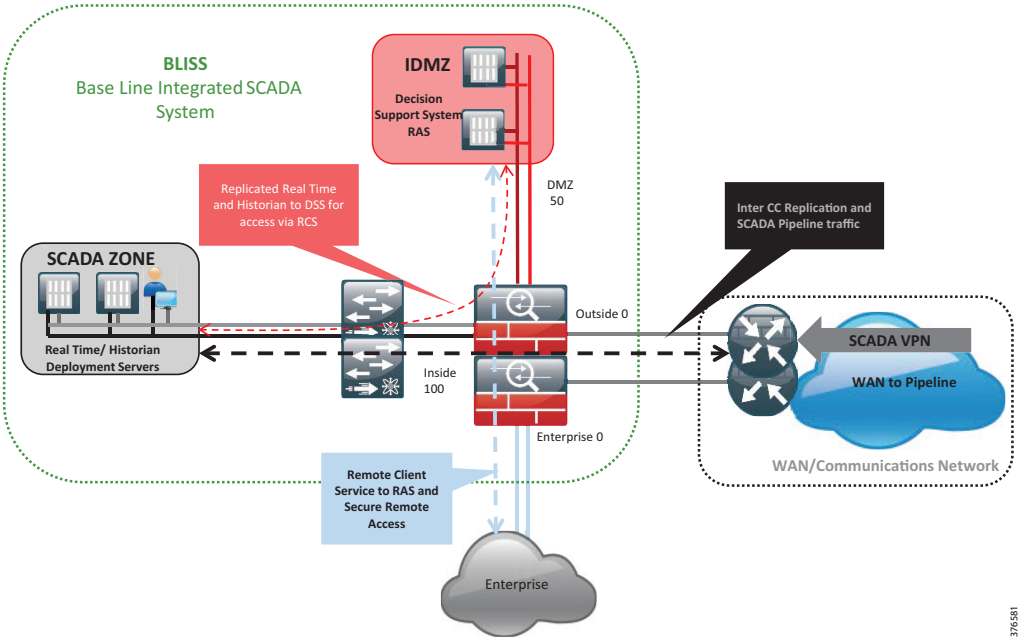
- Each SCADA application works in hot/standby capacity with hot server hosted (for example) on blade 1/chassis 1 while the standby server is hosted on blade 1/chassis 2. Hosting application servers on such a redundant UCSB5108 chassis setup helps ensure redundancy in terms of power/blade/chassis failure.
- Each SCADA application working in hot/standby helps ensure the communication between Control Center and Pipeline Network is primarily handled by hot server with standby waiting to take over in case of a failure scenario. The information from Pipeline Network is mirrored between the hot and standby servers.
- Two Cisco ASR 902s help ensure redundant path from Control Center to Pipeline Network via the MPLS/IP wide area network.
- Two Nexus 3524 switches within the Control Center provide redundant paths for Production and DSS traffic.
- Two ASA 5525-Xs are deployed in a failover setup to provide redundancy.
- Two FI6248 Fabric Interconnects connecting the UCS chassis to Nexus switches provide hardware redundancy.
- Methods like Virtual Router Redundancy Protocol (VRRP) between edge routers, failover link in firewall, vPC in the Nexus switches, Microsoft Hyper-V vSwitch, and redundant Fabric Interconnects provide a fast failover mechanism.
- Multiple VSANs allow for redundant paths from servers to the external storage. A second external storage array would normally be used for storage redundancy; however a second array was not part of this implementation.

Note Backup Control Center was not part of the implementation of the solution.

Security

Figure 1-3 shows traffic patterns within Control Center.

Figure 1-3 Security Design for Control Center



Security within the Control Center is provided through the following methods:

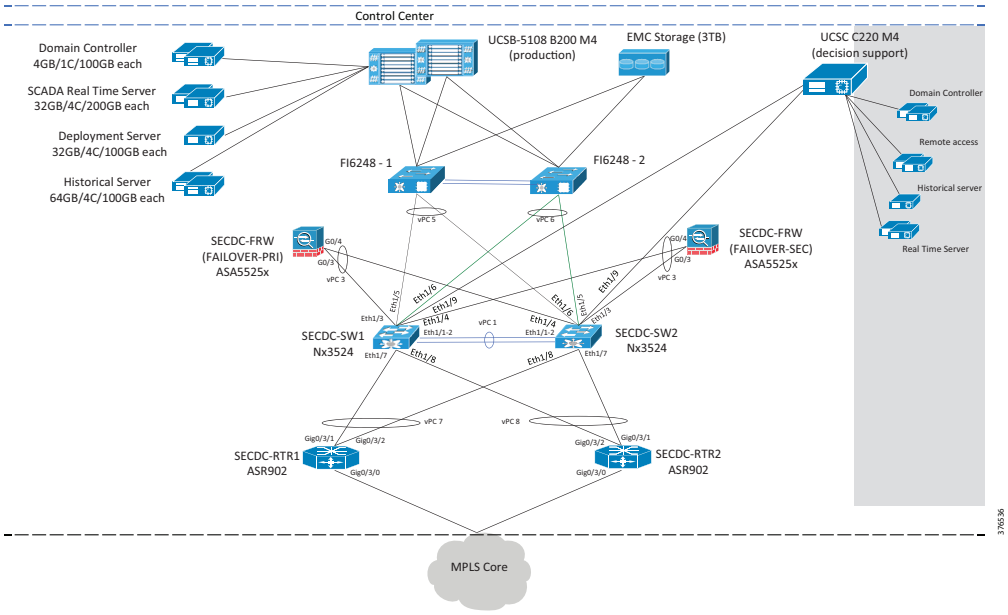
- Separation of Pipeline LAN traffic using separate VRF instances in the edge routers
- Separation of Production and DSS traffic within the Control Center using separate VLANs - VLAN 120 for Production and VLAN 125 for DSS zones
- Access control policy in firewall allowing access only between:
  - Production zone and Pipeline Network segments
  - Production and DSS zones for data replication
  - DSS and Corporate/Enterprise users
- Only necessary ports permitted in access control; all remaining ports denied access
- Cisco AnyConnect Secure Mobility Client installed on the firewall provides secure SSL connections to DSS zone for remote Corporate users
- Unused ports of the access switch are shutdown
- Port security configured on ports connecting operator stations

System Testbed

This chapter describes the Control Center system testbed.

Figure 2-1 provides the system testbed of the Control Center virtualization. Per the design principles, the SCADA application servers in the Production zone are hosted on UCS B200 M4 blade servers on a pair of UCS B5108 chassis for redundancy. The application servers in the Production zone are booted from an external storage array EMC VNxe3200 connected via a pair of FI6248 Fabric Interconnects. This external storage is also used for the Historical server database.

Figure 2-1 System Testbed for Control Center Virtualization



SCADA application servers in the decision support zone are on the UCS C220 M4 rack mount server. These applications are booted from local storage on the UCS C server.

Connectivity within the Control Center between SCADA application servers, operator stations, and firewall are provided by a pair of Nexus 3524 switches.

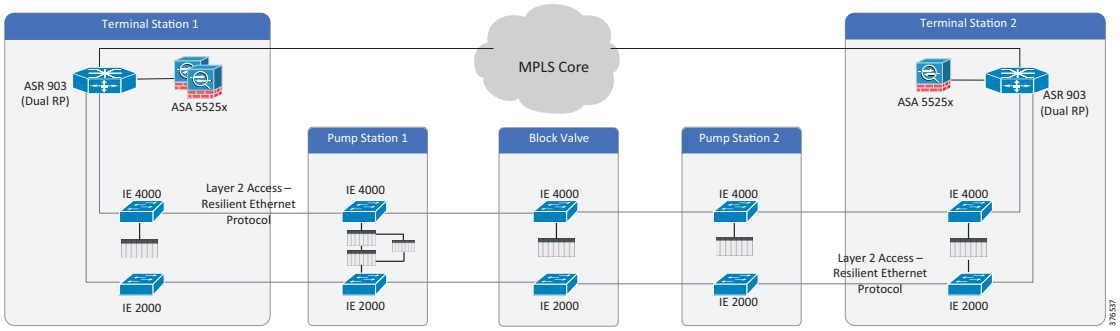
A pair of firewalls (ASA 5525-X) operating in primary/secondary roles act a default gateway for the SCADA application servers. Access control policy configured on the firewall controls the traffic between Pipeline stations and SCADA servers in the Production zone. The policy also controls the traffic between Production and DSS zones within the Control Center.

Connectivity between the Control Center and Pipeline is through a pair of ASR 902 edge routers for redundancy.

The solution components and software matrix for this test bed is listed in Chapter 3, "System Components and Software Matrix."

Note To facilitate the validation of the BLISS Control Center, a representative network of the Pipeline segment was set up in the lab environment (see Figure 2-2). This Pipeline segment terminates at the terminal stations on each end of the Pipeline segment. Intermediate stations such as pump and block-valve stations have Programmable Logic Controllers (PLCs) monitoring the health of the Pipeline. These PLCs are connected to Industrial Ethernet switches within different stations and communicate with the Control Center via MPLS/L3VPN technology. Validation of this Pipeline segment is covered as part of a subsequent Cisco Validated Design.

Figure 2-2 Representative Testbed for Pipeline Segment



System Components and Software Matrix

The Control Center in a Connected Pipeline solution is comprised of the UCS, Data Center switches, firewalls, aggregation routers, and storage array. The units include:

- UCS B5108 blade server chassis
- UCS-IOM-2208XP fabric extenders
- FI6248 Fabric Interconnects
- Nexus 3524 switches
- ASA 5525-X firewall
- ASR 902 aggregation routers
- EMC VNXe3200 storage array

Table 3-1 lists Cisco software components.

Table 3-1 Cisco Software Components

Component	SW Version	Role
UCS B200 M4	2.2.5a	Server to host Production SCADA applications
UCS C220 M4	2.0(6d)	Server to host decision support SCADA applications
FI6248	2.2.5a	Fabric Interconnect (to connect UCS, EMC and nexus)
Nx3548 (Design mentions Nx3524, but Nx3548 was used in implementation)	6.0(2)A4(5)	Data Center switch to connect aggregation router, firewall, UCS C220 M4, operator stations
EMC VNXe3200	3.1.1.5395470	Storage array from where Production servers boot. Also used for Production Historical database.
ASA 5525-X	9.2(3)4	Firewall to decision making between zones within Control Center
Cisco ASR 902	15.5(2)S	Aggregation Series Router for connectivity from Control Center to the Pipeline via MPLS/IP cloud

Table 3-2 lists test components from Schneider Electric.

Table 3-2 Schneider Electric Software Components

Component	SW Version
Windows Server	2012 R2
MS SQL Server	2012 SP1
Visual Studio	2013 Professional
OASyS DNA Elk	SP4 ML 7.7.1
OASyS DNA OGP • LMS: R4.1.1 • Measurement: R5.6 • RealTime Gas: R5.2 • Gas Day Operations: R5.4 • OGX: CR2 • Liquids clients: – LibAPI.Installer.1.0.19 – WebClientInstaller2013.1.0.5 – Liquid.Installer.NET45-1.0.28	7.6

Table 3-3 lists Schneider Electric PLCs.

Table 3-3 Schneider Electric PLCs

PLC and RTU
M340
SCADAPack350
M580

Control Center Virtualization: Implementation

This chapter, which describes how to configure the Control Center for BLISS, is based on the design considerations outlined in the *Control Center Virtualization for the Connected Pipeline System Design Guide*, which can be found at the following URL:

- https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-11217883

The following chapters include configurations that have been validated during the testing effort:

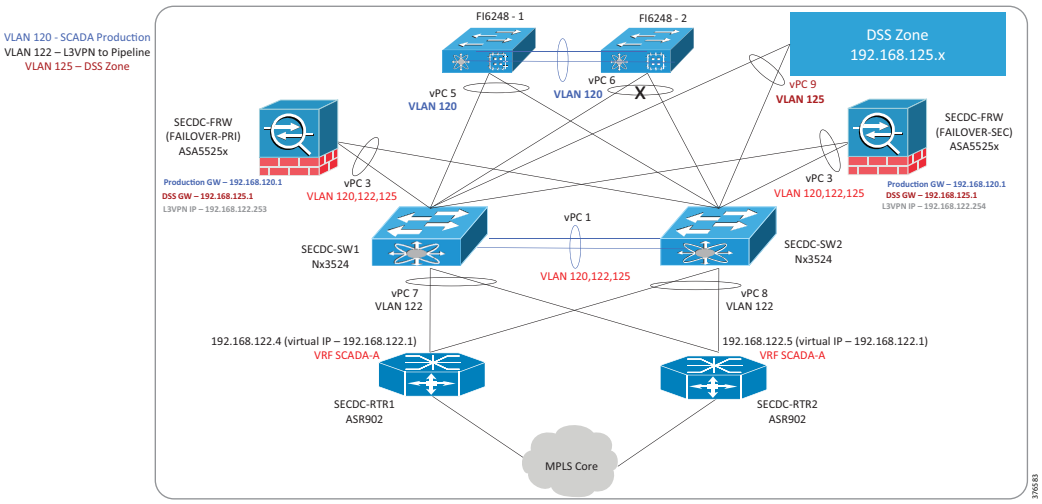
BLISS Implementation

This section describes the configuration and implementation of the BLISS Control Center. The aim of this section is to provide a comprehensive overview and fundamentals of various platforms that fit into the required network, compute, storage and security architecture, implemented features, and configuration to support the BLISS design.

Network

Figure 4-1 depicts how different components within the BLISS are connected.

Figure 4-1 Network Connectivity within Control Center



Aggregation Router Configuration

Note BLISS system design is edge router agnostic. For BLISS validation purposes and to simulate the edge router functionality, Cisco ASRs were utilized. This is only a representation of how such a edge router is configured.

Aggregation router sits at the edge of the Control Center to deliver converged services. It delivers enhanced broadband experience for a variety of services including voice, video, and data. In the BLISS implementation, a pair of aggregation routers are set up to provide redundancy for connectivity between the Control Center environment and the Pipeline Network via a Service Provider Network (sometimes referred as Operational Telecom Network) using MPLS/IP. ASR 902 is the router platform chosen to provide this functionality. With shallow depth, low power consumption, and an extended temperature range, this compact two-rack unit router provides high service scale and flexible hardware configuration.

The access network within the Control Center is segregated into different domains: Production, Test and Development, and DSS. From an integrity and security standpoint, the information from each zone should be kept separate within the realms of the aggregation routers. For this purpose, each network's information is stored in separate VRF instances. The two sets of aggregation routers provide redundancy and advertise the Control Center networks to the operation network and, therefore, an alternate path for the Pipeline stations to reach Control Center applications.

This pair of aggregation routers are connected to a set of access switches (Nexus 3524) within the Control Center using vPCs.

For the purpose of this BLISS implementation, IP address ranges within the Control Center are as follows:

- **Production Zone**—192.168.120.x/24
- **DSS**—192.168.125.x/24

The following is the configuration necessary to communicate with the Service Provider Network (Operational Telecom Network):

Configure the router to use label distribution protocol (LDP) for the MPLS:

```
!
```

```
mpls label protocol ldp
!
```

Loopback interfaces are configured on a router for variety of purposes. Loopback interfaces remain in an operationally *up* state as long as the router is functionally *up*. In this setup, loopback interface is configured and is used as an identifier with MPLS, routing protocols like OSPF and BGP:

```
!
interface Loopback0
 description LOOPBACK_ROUTER_ID
 ip address 192.168.1.4 255.255.255.255
!
```

Configure the interface facing the Service Provider Network router and enable MPLS:

```
!
interface GigabitEthernet0/3/0
 description TO-WAN_CORE::Gig0/0/0
 mtu 9216
 ip address 192.168.20.7 255.255.255.254
 load-interval 30
 negotiation auto
 mpls ip
 cdp enable
!
```

Configure the aggregation router to communicate with the other router within the Control Center and with the Service Provider Network using Open Shortest Path First (OSPF). For exchange of network information between Control Center and Pipeline Networks, configure the router to peer with the other router within the Control Center and with the Service Provider Network using Border Gateway Protocol (BGP).

Note For the implementation of BLISS, *192.168.1.1* and 1*92.168.1.2* are peer routers on two ends of the Pipeline Network. *192.168.1.5* is the second edge router within the Control Center.

```
!
router ospf 1
 router-id 192.168.1.4
 network 192.168.1.4 0.0.0.0 area 0
 network 192.168.20.6 0.0.0.1 area 0
!
!
router bgp 10
 bgp router-id 192.168.1.4
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 10
 neighbor 192.168.1.1 update-source Loopback0
 neighbor 192.168.1.2 remote-as 10
 neighbor 192.168.1.2 update-source Loopback0
 neighbor 192.168.1.5 remote-as 10
 neighbor 192.168.1.5 update-source Loopback0
 !
 address-family ipv4
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.5 activate
 exit-address-family
 !
!
```

Configure the virtual routing and forwarding instances on the router. Necessary configurations under BGP are also included.

```
!
ip vrf SCADA_A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
```

The aggregation router communicates internally within the Control Center via a set of Nexus 3524 switches using port-channels. See Figure 4-1 on page 4-2.

```
!
interface GigabitEthernet0/3/1
 description TO_SECDCSWT::Gig2/0/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 2 mode active
!
interface GigabitEthernet0/3/2
 description TO_SECDCSWT::Gig1/0/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 2 mode active
!
!
interface Port-channel2
 ip vrf forwarding SCADA_A
 ip address 192.168.122.4 255.255.255.0
 vrrp 120 ip 192.168.122.1
 vrrp 120 priority 110
 vrrp 120 preempt
 ip summary-address eigrp 10 0.0.0.0 0.0.0.0
 no negotiation auto
!
```

The access router uses EIGRP as the routing protocol to learn about the Production and DSS networks and advertise the same to the Service Provider Network.

Note This router obtains this information from the firewall assembly acting as the default gateway for the Control Center. This firewall/gateway aspect will be covered in the next section.

```
!
router eigrp 10
 !
 address-family ipv4 vrf SCADA_A
  network 192.168.122.0
  autonomous-system 10
  eigrp router-id 192.168.1.4
 exit-address-family
 !
!
router bgp 10
!
!
 address-family vpnv4
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 send-community extended
```

```
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 send-community extended
  neighbor 192.168.1.5 activate
  neighbor 192.168.1.5 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf SCADA_A
  redistribute connected
  redistribute eigrp 10 route-map SET_MED
 exit-address-family
 !
!
```

In a redundant setup of aggregation routers, one router is configured to operate as primary and the other as the secondary. Production and DSS networks are advertised to the Service Provider Network via the primary router with a better metric compared to the secondary router. Access control lists and route maps are employed for this purpose.

```
!
access-list 1 permit 192.168.110.0 0.0.0.255
access-list 2 permit 192.168.120.0 0.0.0.255
access-list 2 permit 192.168.125.0 0.0.0.255
!
route-map SET_MED permit 10
 match ip address 2
 set metric 100
!
route-map SET_MED permit 20
 match ip address 1
 set metric 200
!
```

Note Configuration of the secondary (or redundant) router will be very similar to that of the primary router.

Access Switch Configuration

In the BLISS implementation, a pair of access switches are set up for connectivity between Fabric Interconnects, firewall, and the edge router (see Figure 4-1 on page 4-2). Nexus 3524 is the Data Center switch platform chosen to provide this functionality.

To support redundant high-available functionality from the two Nexus 3524 switches, a vPC is configured between them. A vPC allows links that are physically connected to two different Nexus switches to appear as a single switch to another device. It hides Spanning Tree-blocked ports and presents a loop-free topology. vPC allows all available bandwidth to be used via multiple links and provides fast-convergence. Having multiple links in a vPC also provides link-level resilience and high availability. A vPC typically carries all the configured VLANs on the switch to provide synchronization. In the current implementation, this vPC link carries the VLANs 120 (Production), 122 (L3VPN), and 125 (DSS).

The two Nexus switches form a peer relationship by virtue of a vPC Peer-to-Peer (P2P) link. This vPC P2P link is used to synchronize states between the peer devices. The vPC P2P link carries control traffic between the switches. In link-failure scenarios, a vPC P2P link also carries Unicast traffic. A vPC P2P link is typically configured using 10G interfaces on the link.

More information on vPC can be found at *Virtual PortChannel Quick Configuration Guide* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/interfaces/602_a1_1/b_N3548_Interfaces_Config_602_A1_1/b_N3548_Interfaces_Config_602_A1_1_chapter_0110.html

And at:

- http://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/vpc_design/vpc_best_practices_design_guide.pdf

In the BLISS Control Center, the two Nexus 3524 switches will appear as a single switch to Fabric Interconnects, firewall, and the aggregation routers providing the redundant switch framework. Port channels are configured on Nexus 3524 interfacing with Fabric Interconnects, firewalls, and aggregation routers. The vPCs are configured as trunk ports and only necessary VLANs are permitted to access Production, DSS zones, and the L3VPN.

The access switch assembly can be used to provide access to operator stations within the Control Center. The ports that are connected to these operator stations are configured as access ports for the relevant VLAN (VLAN 120). All the unused ports are configured for port security and are placed into shutdown mode.

Enable the necessary features on the switch: Layer Aggregation Control Protocol (LACP) (for port-channel protocol), vPC, Unidirectional Link Detection (UDLD), and port security:

```
feature telnet
feature tacacs+
cfs eth distribute
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature port-security
```

Create necessary VLANs for the Production and DSS zones:

Note For the implementation of BLISS, VLAN 120 is the Production LAN, VLAN 125 is the DSS LAN. VLAN 122 is created for the L3VPN between the firewalls and aggregation routers.

```
!
vlan 120
  name SCADA_A
vlan 122
  name L3VPN_SCADA_A
vlan 125
  name CDC_DSS
!
```

Create a vPC domain and peer link between the two Nexus 3524 switches:

```
!
vpc domain 1
  peer-keepalive destination 10.27.1.12 source 10.27.1.11
  delay restore 150
  auto-recovery
!
interface Ethernet1/1
  description TO_SECDCSW2::Eth1/1
  switchport mode trunk
  switchport trunk allowed vlan 120,122,125
  channel-group 1 mode active
  no shutdown
!
interface Ethernet1/2
  description TO_SECDCSW2::Eth1/2
  switchport mode trunk
```

```
  switchport trunk allowed vlan 120,122,125
  channel-group 1 mode active
  no shutdown
!
interface port-channel1
  switchport mode trunk
  switchport trunk allowed vlan 120,122,125
  spanning-tree port type network
  vpc peer-link
!
```

Create port-channels to interface with Fabric Interconnects, firewalls, and aggregation routers. Configure them as vPC. Refer to Figure 6 for a graphical representation of VLAN assignment. Configure the relevant interfaces for port-channels:

Port-Channel towards Firewall:

```
!
interface Ethernet1/3
  speed 1000
  description TO_SECDCFRW1::Gig0/3
  switchport mode trunk
  switchport trunk allowed vlan 120,122,125
  channel-group 3 mode active
  no shutdown
!
interface Ethernet1/4
  speed 1000
  description TO_SECDCFRW2::Gig0/4
  switchport mode trunk
  switchport trunk allowed vlan 120,122,125
  channel-group 4 mode active
  no shutdown
!
interface port-channel3
  description PORTCHANNEL_TO_SECDCFRW
  switchport mode trunk
  switchport trunk allowed vlan 120,122,125
  vpc 3
!
interface port-channel4
  description PORTCHANNEL_TO_SECDCFRW
  switchport mode trunk
  switchport trunk allowed vlan 120,122,125
  vpc 4
!
```

Create port-channel interfaces with Fabric Interconnects (for Production zone):

Note Fabric Interconnect configuration details are covered in Default Gateway Configuration, page 4-9.

```
!
interface Ethernet1/5
  description TO_FI1::int5
  switchport mode trunk
  switchport trunk allowed vlan 120
  channel-group 5 mode active
  no shutdown
!
interface Ethernet1/6
  description TO_FI2::int6
```

```
  switchport mode trunk
  switchport trunk allowed vlan 120
  channel-group 6 mode active
  no shutdown
!
interface port-channel5
  description TO_FABRIC_INTERCONNECT
  switchport mode trunk
  switchport trunk allowed vlan 120
  vpc 5
!
interface port-channel6
  description TO_FABRIC_INTERCONNECT
  switchport mode trunk
  switchport trunk allowed vlan 120
  vpc 6
!
```

Create port-channel interfaces with UCS-C 220 M4 server (for DSS zone):

```
!
interface Ethernet1/9
  speed auto
  description TO_SECDCDSSHV1
  switchport mode trunk
  switchport trunk allowed vlan 125
  channel-group 9 mode active
  no shutdown
!
interface port-channel9
  description Port-Channel to DSS
  switchport mode trunk
  switchport trunk allowed vlan 125
  vpc 9
!
```

Create port-channel interfaces with aggregation routers:

```
!
interface Ethernet1/7
  speed 1000
  description TO_SECDCRTR1::Gig0/3/1
  switchport access vlan 122
  channel-group 7 mode active
  no shutdown
!
interface Ethernet1/8
  speed 1000
  description TO_SECDCRTR2::Gig0/3/2
  switchport access vlan 122
  channel-group 8 mode active
  no shutdown
!
interface port-channel7
  description PORTCHANNEL_TO_SECDCRTR
  switchport access vlan 122
  vpc 7
!
interface port-channel8
  description PORTCHANNEL_TO_SECDCRTR
  switchport access vlan 122
  vpc 8
 !
```

Port-channel interfaces with operator workstations in Production and DSS zones:

```
!
interface Ethernet1/45
  speed 1000
  description OPERATOR_STATION_PRODUCTION
  switchport access vlan 120
  no shutdown
!
interface Ethernet1/46
  speed 1000
  description OPERATOR_STATION_DSS
  switchport access vlan 125
  no shutdown
!
```

Configure all unused ports on the switch for administrative shutdown mode:

```
!
interface Ethernet1/32 description
description UNUSED_PORT
shutdown
```

Note The second Nexus 3524 switch will have a similar configuration except for changes in the port-channel/vPC numbers.

In situations where operator stations are located away from the Control Center, the Control Center network has to be extended. In such a scenario, traditional Catalyst switches like Cisco 3850 are used. Ports connecting to operator stations are configured for port security.

Note An example of only one port configured for port security is shown below. More information on Cisco 3850 port security configuration options can be found at the following URL:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3e/consolidated_guide/configuration_guide/b_consolidated_3850_3e_cg/b_consolidated_3850_3e_cg_chapter_01000110.html

```
interface Ethernet1/32 description
description TO_OPERATOR_STATION
switchport access vlan 120
switchport port-security mac-address sticky
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
```

Default Gateway Configuration

The Cisco ASA5525-X is configured using Adaptive Security Device Manager (ASDM). Information about downloading ASDM version 7.4, install and configuration can be found here -

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/asdm74/firewall/asdm-74-firewall-config.html

In addition to using the Cisco ASA 5525-X as a firewall, the device will also behave as the default gateway for the Production and DSS zones within the Control Center. Refer to Figure 4-1 on page 4-2.

Note This guide assumes that the user has already performed the initial setup and hardening of the Cisco ASA. For more details on these configurations, refer to the following URL:

- http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

The following steps describe the initial configuration of interfaces in the firewall.

Step 1 Configure interfaces for the SCADA Production zone, DSS zone, and L3VPN interface attached to edge routers (See Figure 4-2).

a. Select **Interfaces** within the Device Setup pane.

b. Click **Add** to the right of the interface list, and then choose **EtherChannel Interface**.

c. Enter values for the Port-channel ID and Interface Name fields.

- For the Production zone (SCADA-A) EtherChannel, enter Security Level as 100.
- For the DSS zone EtherChannel, enter Security Level as 100.
- For the L3VPN EtherChannel, enter Security Level as 0.

d. Select the **Enable Interface** option.

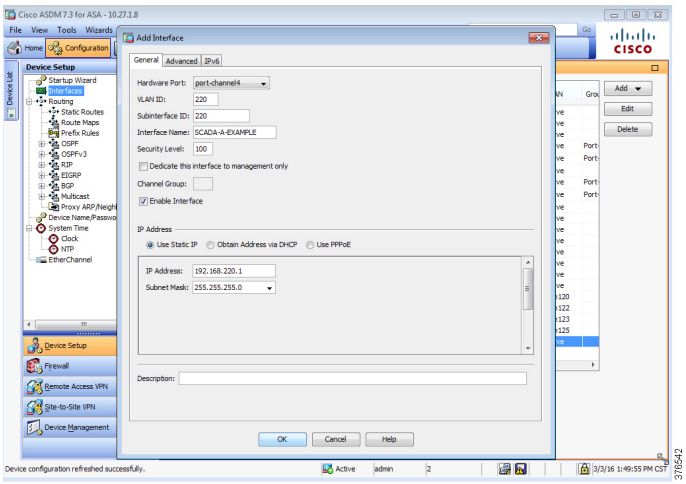
e. Select physical interfaces that should be included within the EtherChannel, and then click **Add**.

f. Select the **Use Static IP** option and enter the IP address and subnet mask for the EtherChannel.

g. If desired, fill in the Description field to help identify the purpose of this EtherChannel, and then click **OK**.

h. Click **Apply** to make all changes take effect.

Figure 4-2 Default Gateway Setup on ASA 5525-X



Step 2 Configure EIGRP as the dynamic routing protocol (see Figure 4-3 and Figure 4-4). This is essential for the firewall and aggregation routers to exchange network reachability information between the Control Center environment and the Pipeline segment.

a. Select **Routing > EIGRP > Setup** within the Device Setup pane.

b. In the Process Instances tab, enter the EIGRP Process number, and then click **Advanced**.

c. For the Router ID field, click either **Automatic** (to assign the highest local IP address as the ID) or **IP Address** (to assign an ID manually). Disable the **Auto-Summary** option and enable the **Log Neighbor Changes** and **Log Neighbor Warnings** options. Leave all other settings as default and then click **OK**.

d. In the Networks tab, define each subnet that should be advertised by EIGRP by clicking **Add** and filling in the IP address and Netmask fields.

e. In the Passive Interfaces tab, select **Suppress Routing Updates on All Interfaces**. This prevents interfaces with IP addresses in the Networks list from attempting to form neighborships with adjacent devices. To add exceptions to this option for the industrial and Enterprise-facing interfaces and allow neighborships to form, click **Add** to select each interface and then click **OK**.

f. To enable authentication between EIGRP neighbors for increased security, select **Interface** under EIGRP in the Device Setup pane. Select the desired interface from the list and click **Edit**. Select **Enable MD5 Authentication**, and then enter a shared secret key value and ID. Finally, click **OK**.

g. To enable summarization of advertised EIGRP routes for increased security and efficiency, select **EIGRP > Summary Address** in the Device Setup pane. Click **Add**, and then enter the summary IP address, Netmask, and interface that will advertise the summary route. Leave the Administrative Distance field blank and then click **OK**.

h. Click **Apply** to make all changes take effect.

Figure 4-3 EIGRP Process Configuration on ASA 5525-X

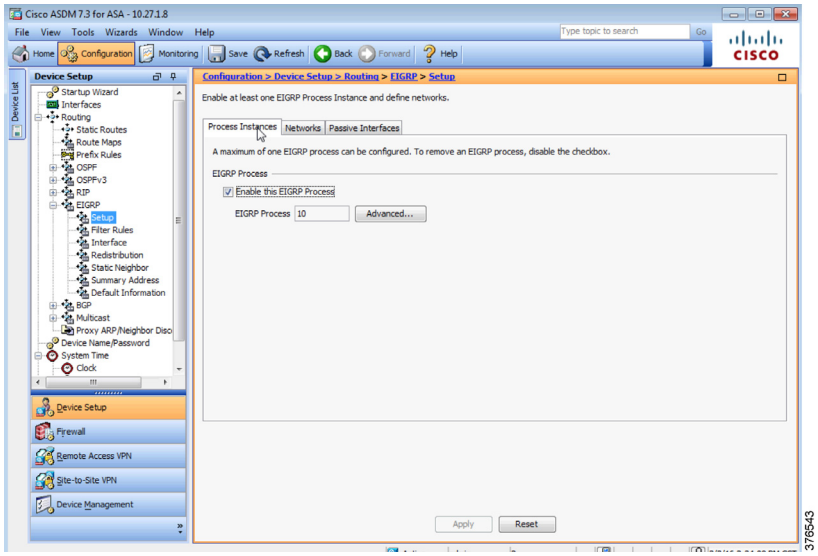
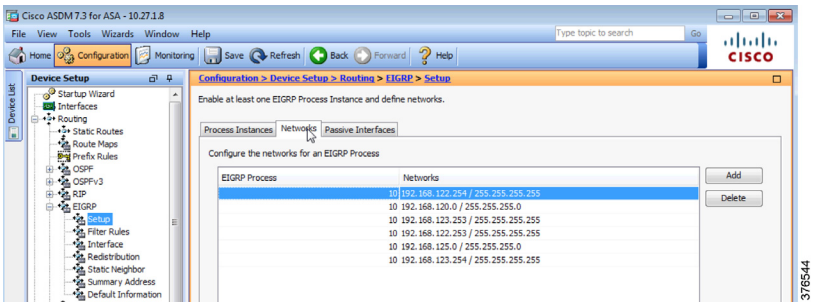


Figure 4-4 EIGRP Process Configuration on ASA 5525-X (continued)



The equivalent CLI configuration for Steps 1-2 is shown below:

```
!
interface GigabitEthernet0/3
 description TO_SECDCSWT::Gig1/0/3
 channel-group 3 mode active
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 description TO_SECDCSWT::Gig2/0/4
 channel-group 3 mode active
 no nameif
 no security-level
 no ip address
!
!
interface Port-channel3
 lacp max-bundle 8
 no nameif
 no security-level
 no ip address
!
interface Port-channel3.120
 vlan 120
 nameif SCADA-A
 security-level 100
 ip address 192.168.120.1 255.255.255.0 standby 192.168.120.2
!
interface Port-channel3.122
 vlan 122
 nameif L3VPN-SCADA-A
 security-level 0
 ip address 192.168.122.253 255.255.255.0 standby 192.168.122.254
!
interface Port-channel3.125
 vlan 125
 nameif CDC_DSS
 security-level 100
 ip address 192.168.125.1 255.255.255.0 standby 192.168.125.2
!
!
router eigrp 10
 auto-summary
 eigrp router-id 10.27.1.8
 network SCADA-A 255.255.255.0
 network CDC_DSS 255.255.255.0
```

```
 network 192.168.122.253 255.255.255.255
 network 192.168.122.254 255.255.255.255
!
```

Compute

This section includes Compute configurations.

Initial Fabric Interconnect Configuration

The Fabric Interconnects house the software that allows for blade configuration and access via the Unified Computing System Manager (UCSM). In order to be able to connect to the UCSM for advanced configurations, the Fabric Interconnects must have some initial configuration via command line. This initial configuration is done through the *Basic System Configuration Dialog*, an example of which can be seen below. This needs to be done for both Fabric Interconnects individually.

```
---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of the system. Only
minimal configuration including IP connectivity to the Fabric interconnect and its
clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system. To back track or
make modifications to already entered values, complete input till end of section and
answer no when prompted to apply configuration.

Enter the configuration method. (console/gui) ? console

Installer has detected the presence of a peer Fabric interconnect. This Fabric
interconnect will be added to the cluster. Continue (y/n)? y

Enter the admin password of the peer Fabric interconnect:  Schn31d3r!
  Connecting to peer Fabric interconnect... done
  Retrieving config from peer Fabric interconnect... done
  Peer Fabric interconnect Mgmt0 IPv4 Address: 10.27.2.3
  Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.0.0
  Cluster IPv4 address          : 10.27.2.2

Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4
Address

Physical Switch Mgmt0 IP address: 10.27.2.4

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

Applying configuration. Please wait.

Configuration file - Ok
```

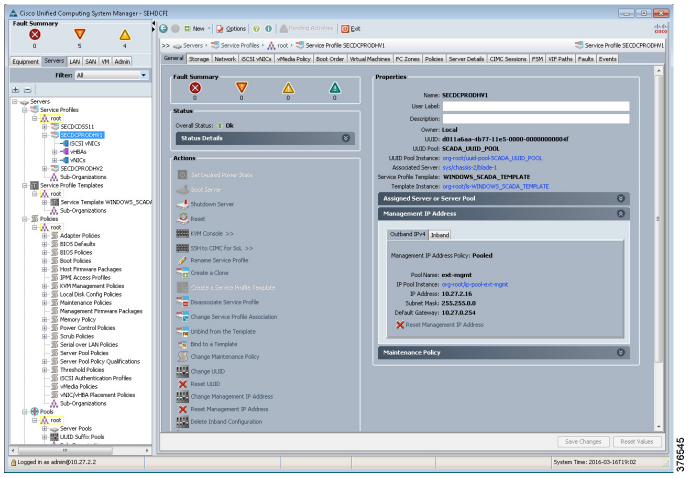
Service Profile Configuration

The service profiles are what provide a given blade with all of the resources it needs to be used as a server. These can be created from a single service profile template for ease of configuration.

Management IP

In order to be able to access the server, the service profile must be associated with a management IP address on the same subnet as the Fabric Interconnect management interface (see Figure 4-5).

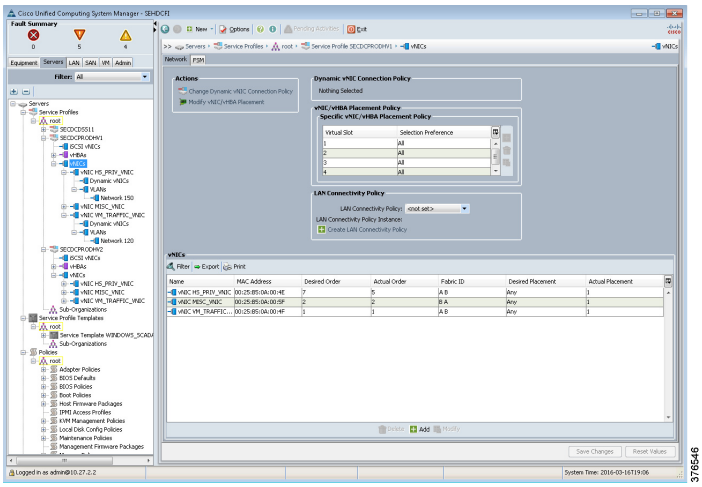
Figure 4-5 Server Management IP Address for Computing



Network Interface Cards

One vNIC is needed for virtual machines/Pipeline communication, while a second vNIC is needed for private communication between historical servers (see Figure 4-6).

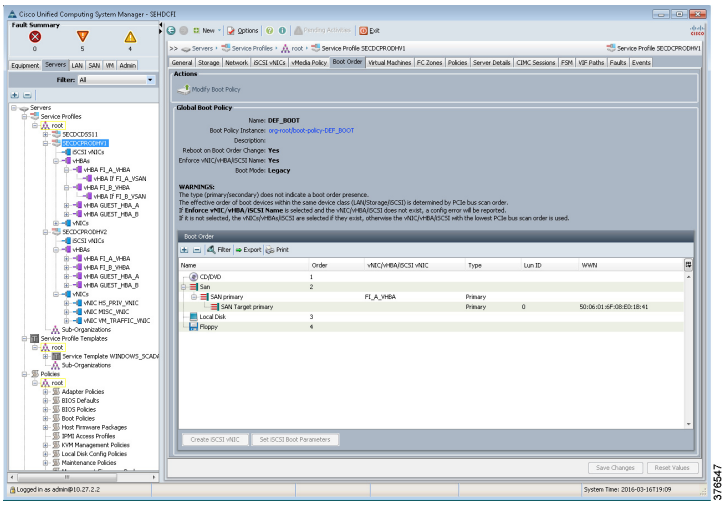
Figure 4-6 Server vNICs



Boot Order

The boot order needs to be configured to allow for boot from both SAN (Windows boot after installation) and from local CD (initial installation). Refer to Figure 4-7 for server boot order.

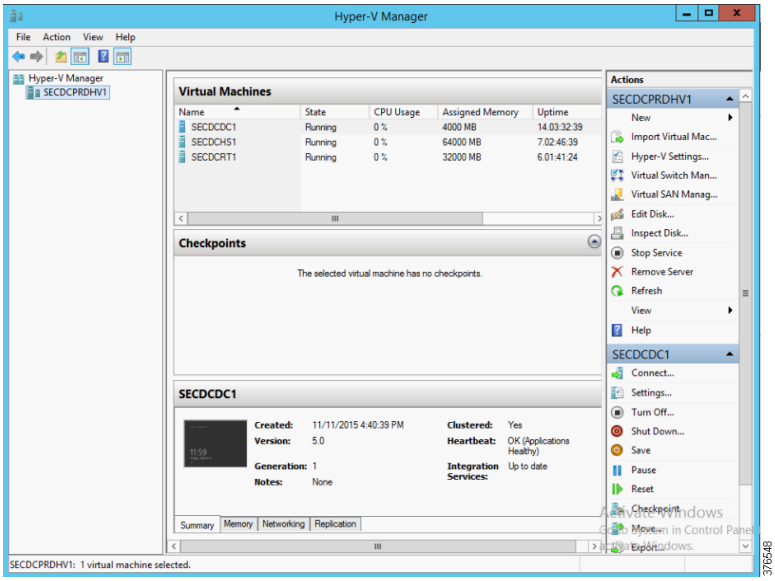
Figure 4-7 Server Boot Order



Microsoft Hyper-V

The hypervisor in this architecture is Microsoft Hyper-V. The Hyper-V software comes by default on the Windows 2012 server; however, it still needs to be installed as a feature using the *Server Manager* tool. Once installed, the Hyper-V manager is used to create virtual machines, virtual switches, and virtual storage networks (see Figure 4-8).

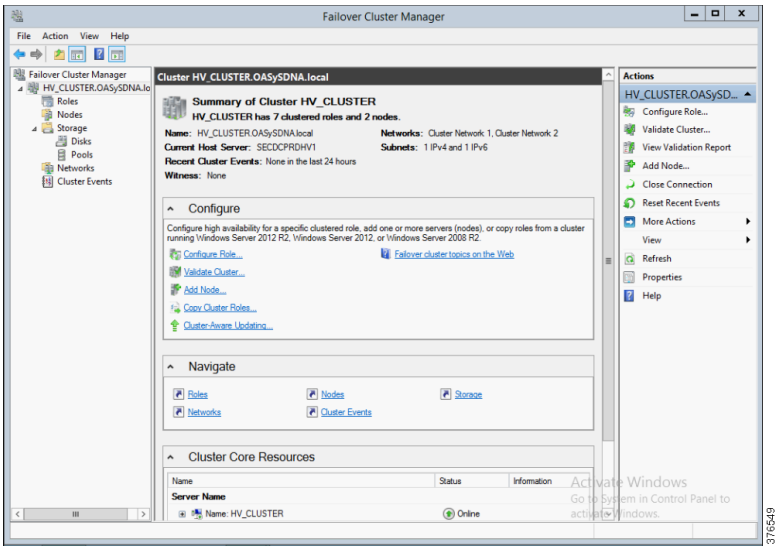
Figure 4-8 Microsoft Hyper-V Manager



Windows Failover Cluster

In addition, the Windows Failover Cluster must be installed in order to cluster the Hyper-V servers together. The Hyper-V servers need to be a part of a cluster in order to share storage between them for some of the virtual machines (see Figure 4-9).

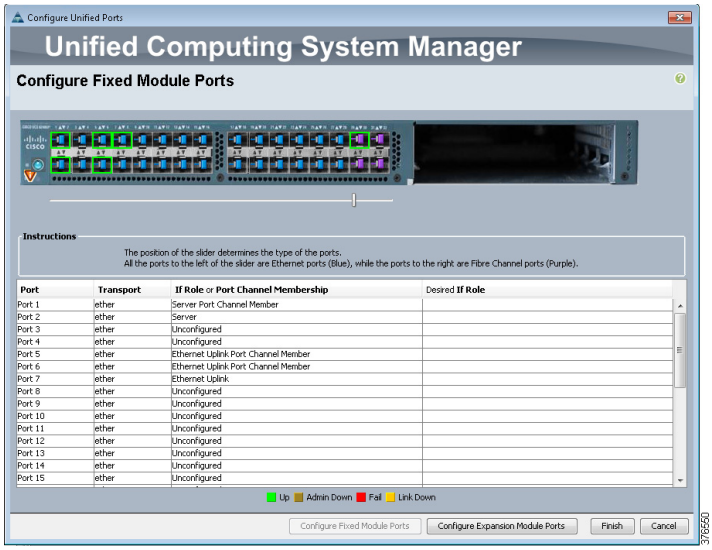
Figure 4-9 Windows Failover Cluster Manager



Storage

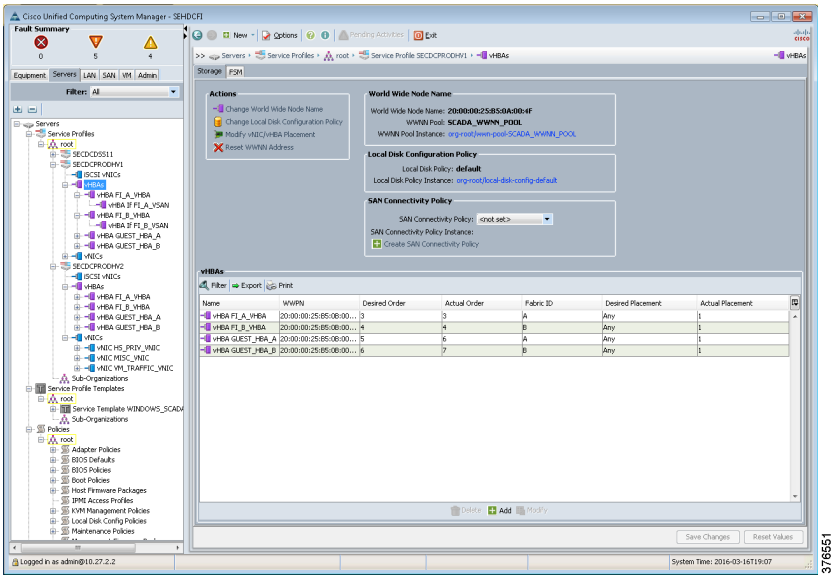
The ports in the Fabric Interconnect are unified, so it is important to configure the necessary ports as Fiber Channel for storage. These ports are connected directly to the EMC storage, with the Fabric Interconnect serving as the *fabric switch* (see Figure 4-10).

Figure 4-10 Unified Port Configuration



In order for the blades to be able to communicate with the EMC storage, Host Bus Adapters (HBAs) must be provisioned. Two HBAs must be allocated per blade for redundancy, and this can be done as a part of the service profile template (see Figure 4-11).

Figure 4-11 Server Virtual HBA Provision



Security

To maintain the integrity and security of the SCADA traffic within the Control Center, a redundant firewall setup is deployed. The function of the firewall is to keep traffic from Production and DSS zones separate. Per the design, Pipeline station devices like Remote Terminal Units (RTUs) and PLCs will be communicating only with the Production zone applications like RealTime servers, deployment servers, and historical servers. They do not directly communicate with the DSS zone.

Enterprise users access relevant SCADA information by gaining access to server instances in the DSS zone in order to restrict direct communication with the field devices. Replication of data between the Production and DSS zones is handled at the application level.

The Cisco ASA platform is deployed in the Control Center to provide firewall capability for security. Access control policies are set up on the firewall to allow access between the following zones:

- Production zone and Pipeline stations
- Production zone and DSS zone
- Enterprise/Corporate to DSS Zone (for remote access capability)

Note Traffic from interfaces with a lower security level to interfaces with a higher security level is implicitly denied by default. However, to confirm complete isolation of all zones and prevent confusion, the user should overwrite these implicit rules with explicit ones.

Configure explicit rules between all zones and apply on the relevant interface (see Figure 4-12)

Step 1 Select **Access Rules** within the Firewall pane.

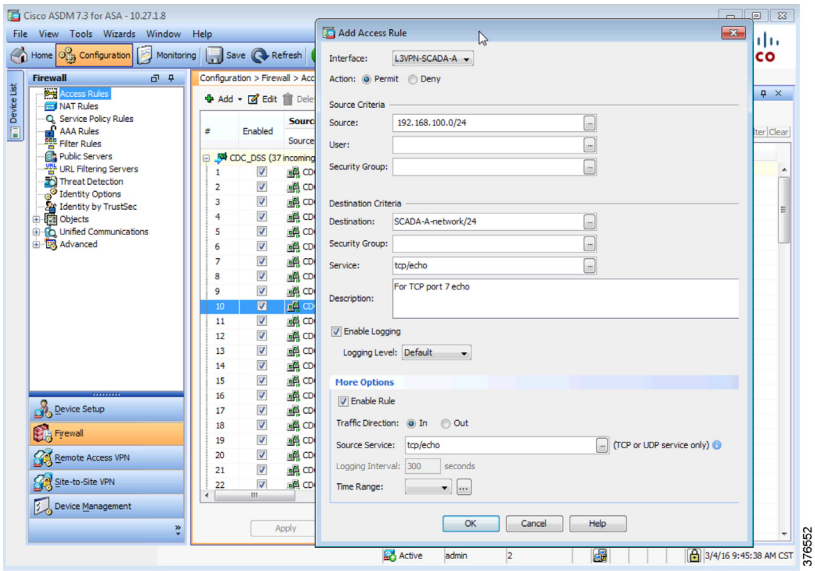
Step 2 For each interface, right-click the interface name and then select **Add Access Rule**.

Step 3 Create a Deny rule with Source as Any and Destination as Any, and then click **OK**.

Step 4 Click the new rule, and then click **Move Down** (down arrow) at the top of the pane until the rule is at the bottom of the interface rule list. Since firewall rules are evaluated in order, the Deny All rule must be at the bottom to only deny traffic that does not match any permit rules for the interface.

Step 5 Click **Apply** to make all changes take effect.

Figure 4-12 Access Control Configuration on ASA 5525-X



Note Figure 4-12 and the configuration steps indicated above are only examples of how to configure access rules on the firewall using ASDM. The access control policy is driven by Schneider's (or the customer's) confidential document. Due to the confidential nature of port names and numbers only the representation used during validation is shown below (CLI).

```
!
access-list 101 extended permit ip <pipeline-scada-a-network> <control-center-network>
access-list 101 extended deny all
!
access-list 102 extended permit <tcp|udp> <control-center-production>
<control-center-DSS> <necessary-protocols>
access-list 102 extended deny all
!
 access-list 103 extended permit <tcp|udp> <control-center-DSS>
<control-center-production> <necessary-protocols>
access-list 103 extended deny all
!
access-group 101 in interface L3VPN-SCADA-A
access-group 102 in interface SCADA-A
access-group 103 in interface CDC_DSS
!
```

Security Implementation

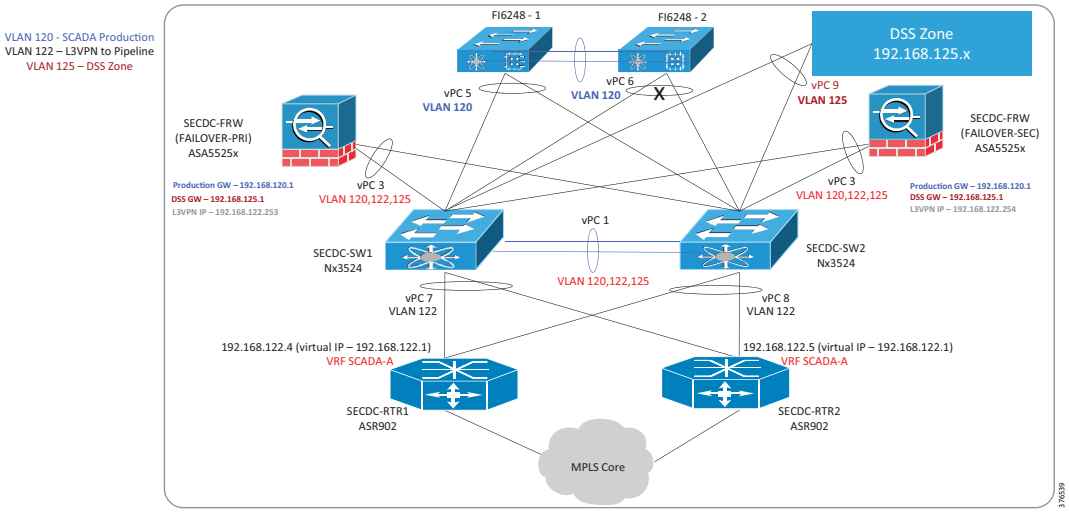
This section includes Security configurations.

Control Center Segmentation and Zones

The BLISS Control Center for the Connected Pipeline will incorporate different zones, namely Production, Test and Development, and DSS (sometimes called the Industrial De-militarized Zone or IDMZ). In the current implementation, the Production zone is hosted on the UCS B200 M4 blade servers on redundant chassis providing hardware segmentation between active and standby application servers. The DSS application servers (active and standby) are hosted on a UCS-C C220 M4 rack-mounted servers. Both these zones have their default gateway setup on the firewall, which has policy enabled that decides the level of granularity in communication between these two zones. The policy defined in firewall allows only application servers in the Production zone to communicate with the Pipeline Network segment. See Figure 4-13.

Note The Test and Development zone is not currently implemented.

Figure 4-13 Control Center Segmentation



Layer 2 Network Segmentation

To facilitate Layer 2 segmentation within the Control Center, the following VLANs were identified:

- **Production Zone**—VLAN 120
- **DSS**—VLAN 125

Figure 4-13 outlines the VLAN segmentation within the Control Center environment. Trunk ports configured on the Nexus 3524 switch are part of a vPC and use 802.1q encapsulation. Although the underlying physical interfaces in a port-channel are common to different zones, separate tagging and encapsulation provides segmentation of traffic. It is possible to have separate physical links for dedicated segmentation of the Production zone, but this not currently implemented.

!

```
interface port-channel5
  description TO_FABRIC_INTERCONNECT
  switchport mode trunk
  switchport trunk allowed vlan 120,125
  vpc 5
!
Nx3548-SECDCSW1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
5     Po5(SU)     Eth      LACP      Eth1/5(P)



Nx3548-SECDCSW1# show interface Ethernet 1/5 status

--------------------------------------------------------------------------------
----
Port          Name               Status    Vlan      Duplex  Speed   Type
--------------------------------------------------------------------------------
----
Eth1/5        TO_FI1::int5       connected trunk     full    10G     SFP-H10GB-CU3M


Nx3548-SECDCSW1# show interface Ethernet 1/5 capabilities
Ethernet1/5
  Model:                 N3K-C3548P-10G-SUP
  Type (SFP capable):    SFP-H10GB-CU3M
  Speed:                 100,1000,10000,40000,auto
  Duplex:                full
  Trunk encap. type:     802.1Q
  Channel:               yes
>> snip <<
```

Layer 3 Network Segmentation

In the BLISS Control Center implementation, the firewall also acts as the default gateway for the Production, Test and Development, and DSS zones. Inter-zone communication will have to traverse this Layer 3 boundary on the firewall and respect policy defined within the firewall.

The interfaces on the firewall are configured to participate in a port-channel. Sub-interfaces are configured on this port-channel for the Production and DSS zones and L3VPN towards edge routers.

For the current implementation, the following IP address ranges were used within the Control Center:

- **Production Zone**—192.168.120.0/24
- **DSS Zone**—192.168.125.0/24
- **L3VPN towards WAN Edge Routers**—192.168.122.0/24

An example configuration of the interfaces is shown below. One of the port-channel sub-interfaces is configured to participate in the Production zone (indicated by SCADA-A). Another sub-interface is configured for the DSS zone, while the other is configured to participate in communication with WAN edge routers indicated by L3VPN-SCADA-A.

```
!
interface Port-channel3.120
 vlan 120
 nameif SCADA-A
 security-level 100
 ip address 192.168.120.1 255.255.255.0 standby 192.168.120.2
!
!
interface Port-channel3.125
 vlan 125
 nameif CDC-DSS
 security-level 100
 ip address 192.168.125.1 255.255.255.0 standby 192.168.125.2
!
!
interface Port-channel3.122
 vlan 122
 nameif L3VPN-SCADA-A
 security-level 0
 ip address 192.168.122.253 255.255.255.0 standby 192.168.122.254
!
```

The firewall participates in an internal gateway routing protocol (like Enhanced Interior Gateway Routing Protocol or EIGRP) with the WAN edge routers for relaying Control Center network information to the Pipeline stations.

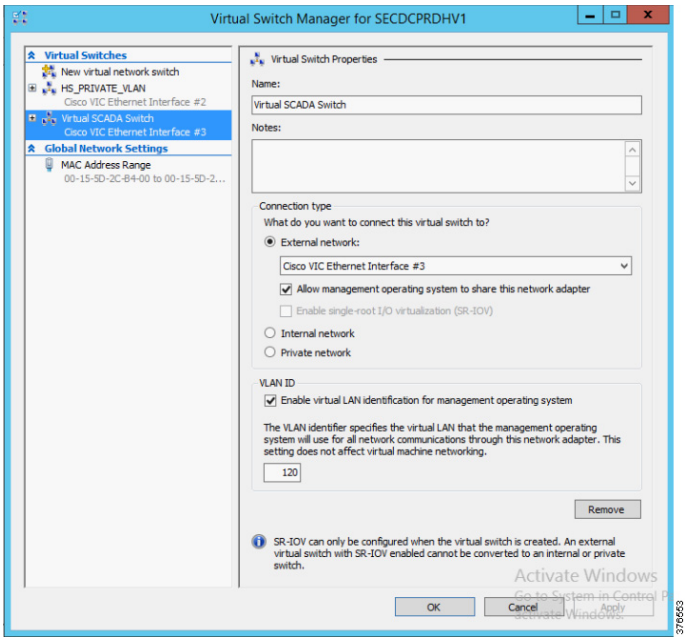
```
!
router eigrp 10
 auto-summary
 eigrp router-id 10.27.1.8
 network 192.168.120.0 255.255.255.0
 network 192.168.125.0 255.255.255.0
 network 192.168.122.253 255.255.255.255
 network 192.168.122.254 255.255.255.255
!
```

The two WAN edge routers participate in a LAN redundancy protocol such as VRRP.

Compute Segmentation

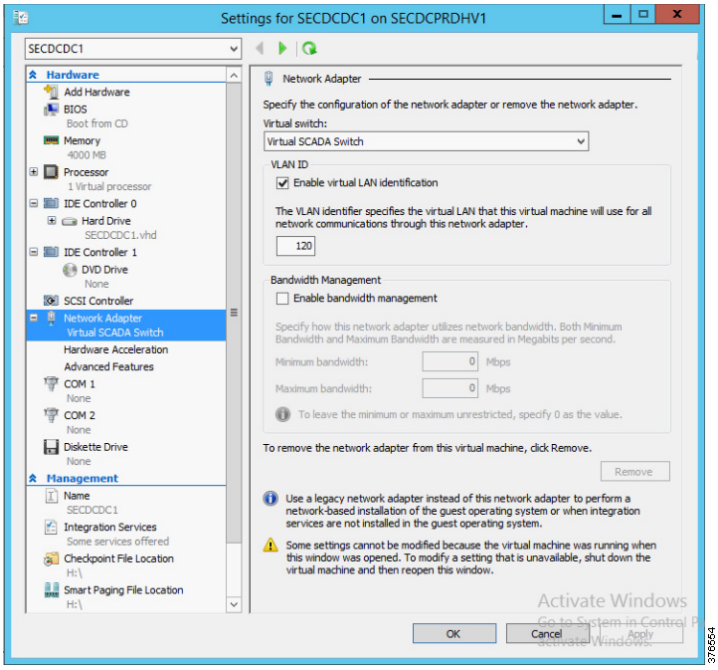
For the virtual machines to be able to communicate with each other (and with the Pipeline), a virtual switch is created in the Hyper-V Virtual Switch Manager. This virtual switch is mapped to a physical network interface card (NIC) on the Hyper-V server (see Figure 4-14).

Figure 4-14 Hyper-V Virtual Switch Manager



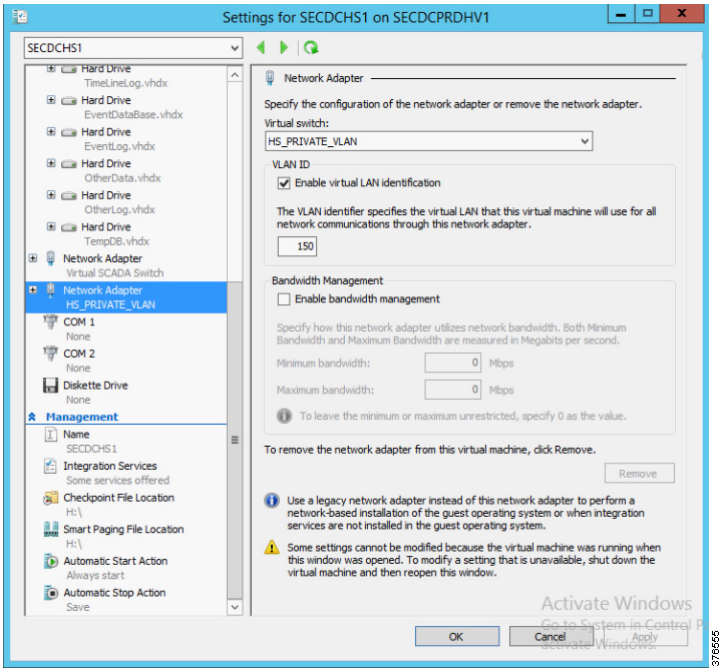
When a virtual machine is created, a virtual Network Interface Card (vNIC) needs to be associated with it. This vNIC is then mapped to the virtual machine in Hyper-V Manager. Once both of these things have been accomplished, traffic can flow between the vNIC on the virtual machine and the physical NIC that is mapped to the virtual switch (see Figure 4-15).

Figure 4-15 Virtual Machine vNIC



In addition, the historical servers need to communicate on a second private VLAN. In Hyper-V Manager, another virtual switch must be created and associated with the physical NIC dedicated for private historical server traffic (see Figure 4-16). When the historical servers are created, a second vNIC must be assigned and mapped to this new virtual switch in the same manner.

Figure 4-16 Historical Server VNICs



Storage Segmentation

This section includes information about storage segmentation.

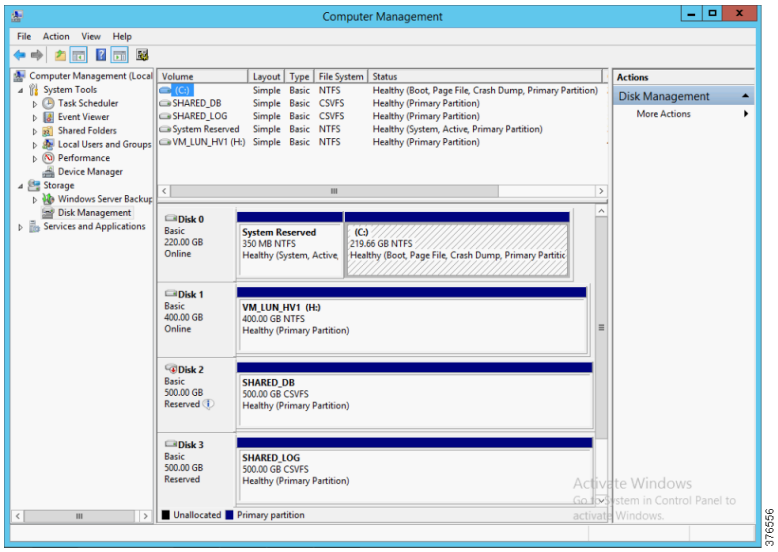
File System Management

Every virtual machine has one or more associated Virtual Hard Disks (VHDs). Each of the VHDs must be stored in a volume owned by the Hyper-V server. This mapping is done in Hyper-V Manager as part of the virtual machine creation (or added posthumously if the VHDs are not ready at the time the virtual machine is created).

Refer to Figure 4-17 for Hyper-V server volume configuration. Each Hyper-V Server has four different volumes that have been allocated via external storage:

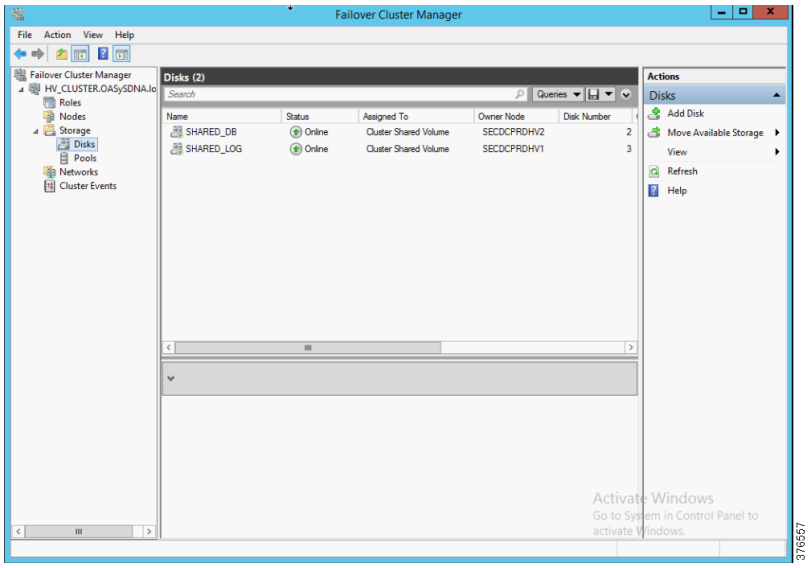
1. A volume that serves as the Hyper-V server's own boot drive
2. A volume for storage of the virtual machines' virtual hard disks
3. A Cluster Shared Volume (CSV) for storage of the historical server VHDs pertaining to database information
4. A CSV for storage of the historical server VHDs pertaining to logging information

Figure 4-17 Hyper-V Server Volumes



The logging and database VHDs need to be stored in a CSV in order for the historical servers (located on different Hyper-V servers) to have concurrent read/write access to them (see Figure 4-18).

Figure 4-18 Cluster Shared Volume



To create a CSV, the Hyper-V servers must be a part of the same two-node failover cluster using the Hyper-V Failover Cluster Manager. The hardware requirements, software requirements, and steps to setting up the cluster itself can be found at *Hyper-V: Using Hyper-V and Failover Clustering* at the following URL:

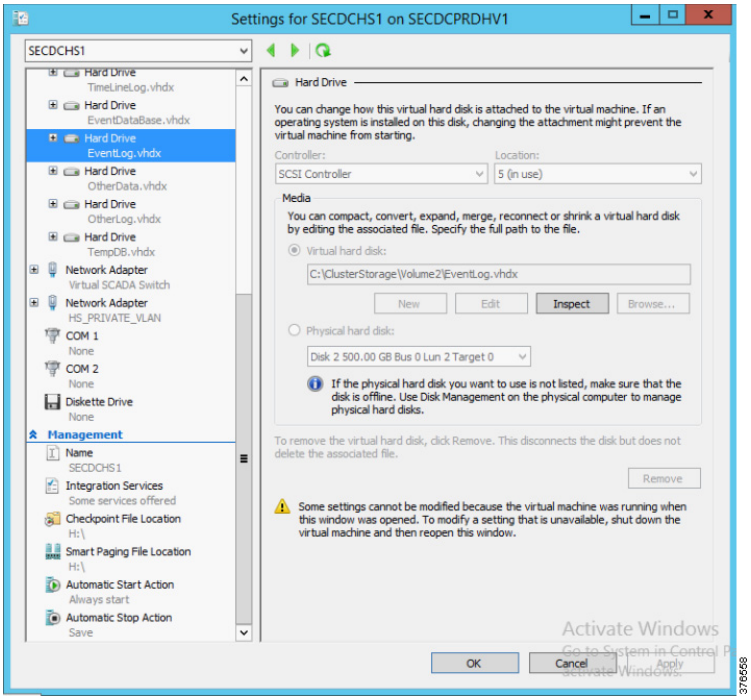
- https://technet.microsoft.com/en-us/library/cc732181(v=ws.10).aspx

After the cluster has been established, hardware requirements, software requirements, and installation steps for creating a CSV can be found at *Use Cluster Shared Volumes in a Failover Cluster* at the following URL:

- https://technet.microsoft.com/en-us/library/jj612868.aspx

Once the CSVs have been created, the additional VHDs that the historical servers require can be stored here as normal (see Figure 4-19).

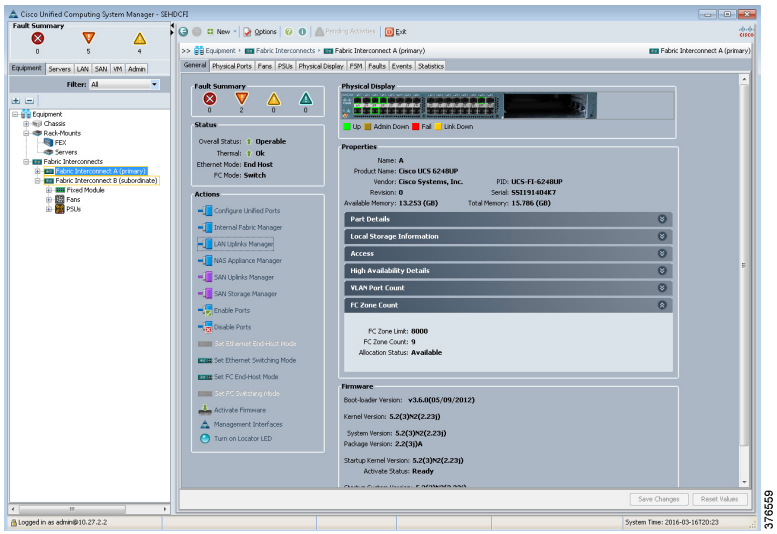
Figure 4-19 Additional Historical Server Drives



Fiber Channel Zoning and VSANs

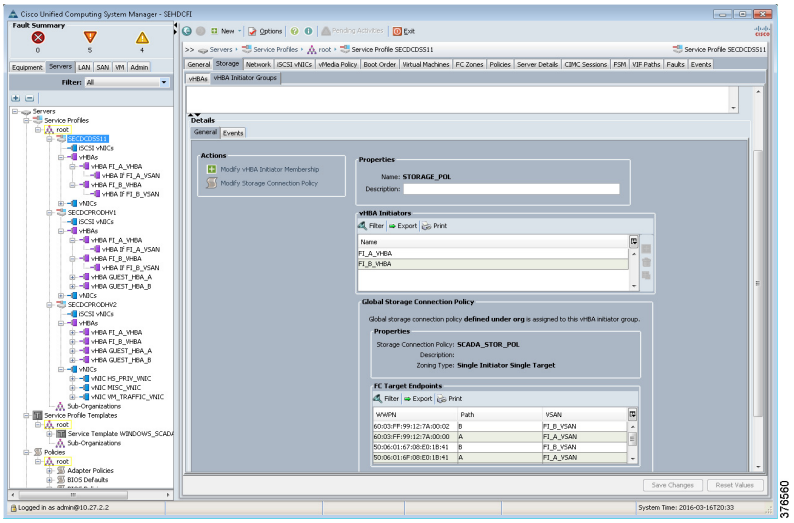
Fiber Channel zoning is performed by the *fabric* in order to control which initiator and target World Wide Port Names (WWPNs) are allowed to communicate with each other (see Figure 4-20). In this environment, the Fabric Interconnects serve as the *fabric* and, as such, must be configured for Fiber Channel switching.

Figure 4-20 Fiber Channel Switching Mode for Zoning and VSANs



Each Hyper-V server must be allocated two HBAs, each of which is zoned for a single target. In addition, the HBAs are associated with different VSANs in order to ensure redundant paths exist from the servers to the storage (see Figure 4-21).

Figure 4-21 Zoning



LUN Masking

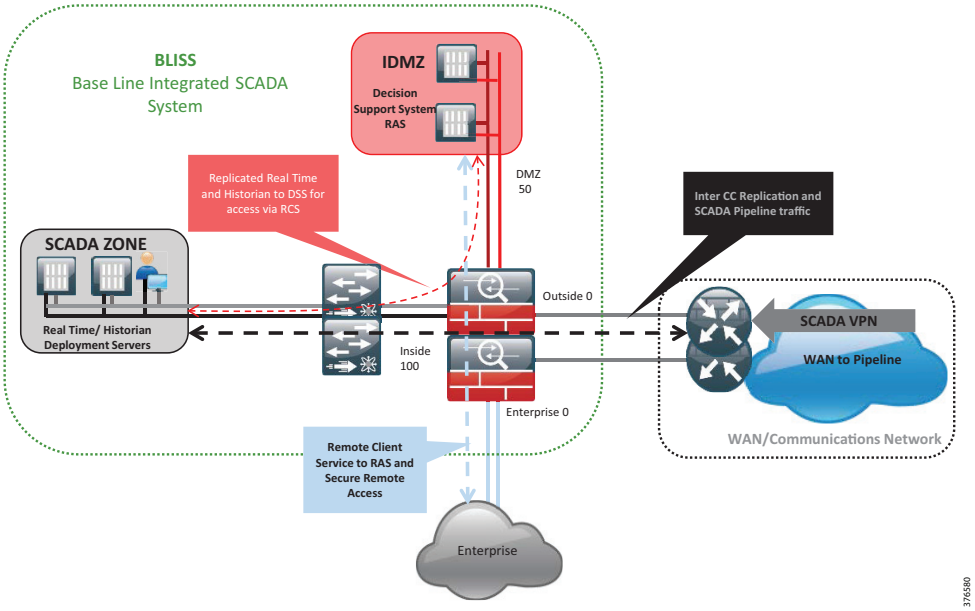
It is important to allow only the requisite Hyper-V servers to have access to a given LUN. This is done via Logical Unit Number (LUN) masking (on the external storage side) where a LUN is made available to a given host. This way, any host that tries to connect to a LUN that has not given it permission will be unable to do so.

For the LUNs that represent a volume that will be turned into a CSV, the LUN must be made available to both nodes in the Hyper-V cluster.

Firewall and Industrial DMZ Implementation

Figure 4-22 shows the firewall setup in the Control Center. A pair of ASA 5525-Xs are set up in redundant hot/standby mode to act as a single consolidated firewall to provide policy for all communication.

Figure 4-22 Firewall in Control Center



The firewall in the Control Center acts as a security boundary for all communication between the following:

- Control Center and Pipeline Network segment
- Different zones (Production, DSS, and Test and Development)
- Enterprise network and Control Center (Industrial DMZ)

Industrial DMZ

In the current implementation, the DSS zone also acts as the IDMZ providing data exchange between the untrusted Enterprise network and the trusted Control Center network. Data replication between application servers in Production and DSS zones allows Enterprise users to access real-time system statistics for monitoring.

The Production zone has RealTime, Historical, Logging, and Deployment servers. Data from these servers are replicated to their counterparts in the DSS zones with the exception of the deployment server. The deployment server is not a part of DSS zone.

The Enterprise users will not be able to directly interact with Control Center network applications nor the Pipeline Network segment.

Policy

The policy setup in the firewall is implemented to allow only pre-defined TCP/UDP ports. All remaining traffic is denied. An example configuration of policy in the firewall follows:

Note Due to the confidential nature of the port-numbers, only a representation is indicated below.

```
!
access-list 101 extended permit ip <pipeline-scada-a-network> <control-center-network>
access-list 101 extended deny all
!
access-list 102 extended permit <tcp|udp> <control-center-production>
<control-center-DSS> <necessary-protocols>
access-list 102 extended deny all
!
 access-list 103 extended permit <tcp|udp> <control-center-DSS>
<control-center-production> <necessary-protocols>
access-list 103 extended deny all
!
access-group 101 in interface L3VPN-SCADA-A
access-group 102 in interface SCADA-A
access-group 103 in interface CDC_DSS
!
```

Security Levels

Firewall interfaces are configured for security levels to define the trust level. Security levels are configured as follows:

- Production zone interface with higher level security (level 100)
- DSS zone interface with higher level security (level 100)
- L3VPN interface towards WAN with lower level security (level 0)

Traffic from higher security level to lower is by default permitted. Traffic from lower security level to higher requires access control policy to be applied in the inbound direction.

```
!
interface Port-channel3.120
 vlan 120
 nameif SCADA-A
 security-level 100
 ip address 192.168.120.1 255.255.255.0 standby 192.168.120.2
!
interface Port-channel3.122
 vlan 122
 nameif L3VPN-SCADA-A
 security-level 0
 ip address 192.168.122.253 255.255.255.0 standby 192.168.122.254
!
interface Port-channel3.125
 vlan 125
 nameif CDC_DSS
 security-level 100
 ip address 192.168.125.1 255.255.255.0 standby 192.168.125.2
!
```

VLAN Segmentation

Servers within the Control Center environment are isolated by VLAN segmentation:

- **Production Zone**—VLAN 120
- **DSS Zone**—VLAN 125

- **L3VPN towards WAN Edge**—VLAN 122

Remote Access

A user can access the SCADA servers in the DSS zone. To provide such an access, one of the following remote access methods is provisioned on the firewall located in the Control Center.

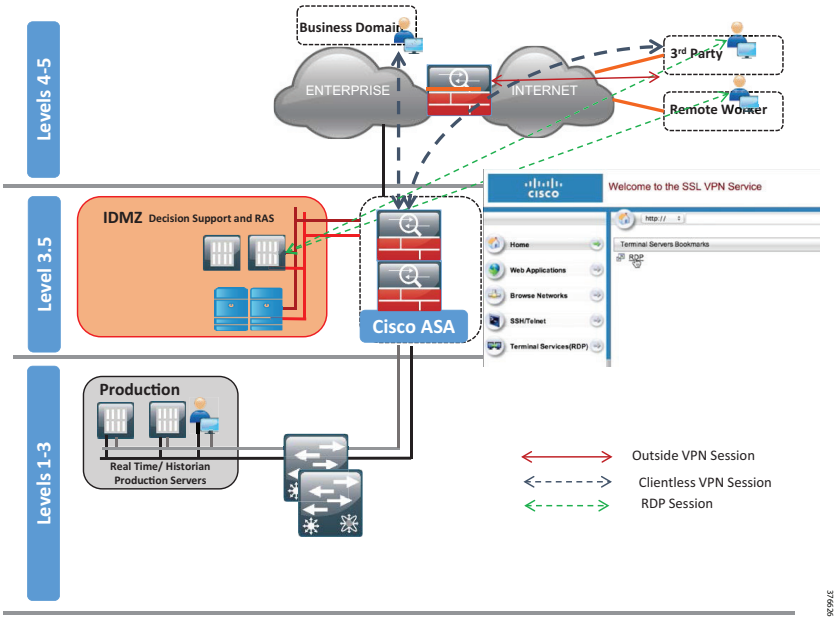
Clientless VPN

The firewall is set up with the Clientless VPN feature with Secure Socket Layer (SSL) encryption. This provides a user the ability to access the DSS zone via web browser without downloading or installing a VPN client on his or her personal computer.

This scenario is specifically mentioned for a user located outside of the enterprise network, like a third party or remote worker trying to gain access to DSS zone over the Internet. The user is expected to first use VPN (outside) to access the corporate network before accessing DSS via web browser (Clientless SSL VPN). Once the SSL VPN session is authenticated, the user will be able to access servers in the DSS zone via RDP. Refer to Figure 4-23.

Necessary ports are opened on the firewall for the enterprise user to communicate with servers in the DSS zone.

Figure 4-23 Remote Access using Cisco SSLVPN (Third Party or Remote Worker)



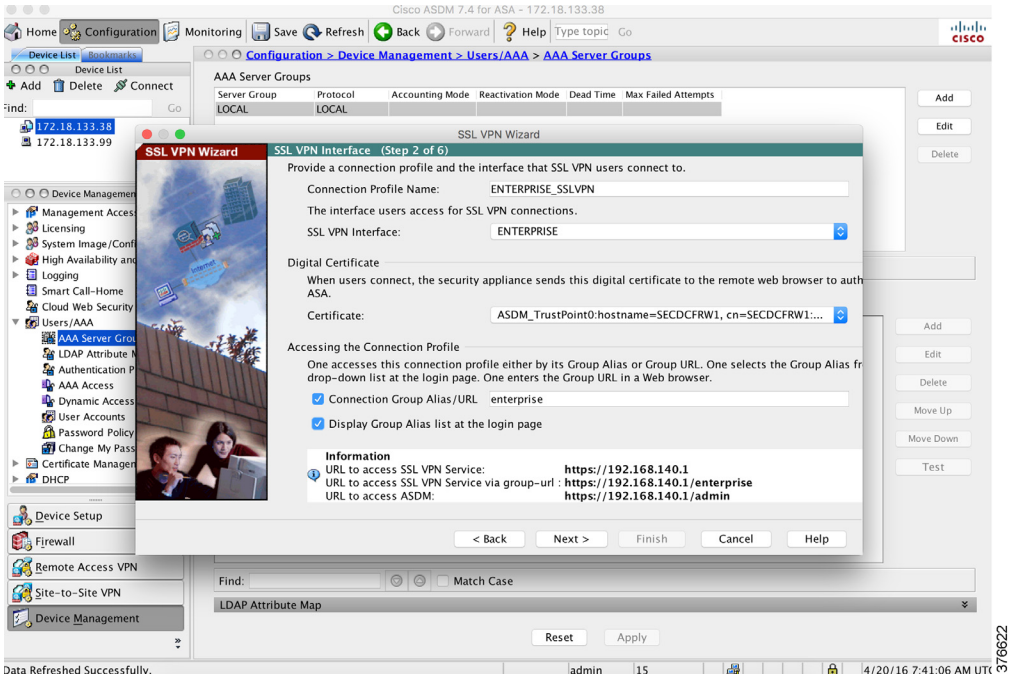
Step 1 Configure the Clientless SSLVPN feature on the ASA5525x using the wizard. Navigate to **Wizards > VPN Wizards > Clientless SSL VPN Wizard**.

Provide the following necessary information for the configuration:

- Profile Name
- Interface on which to accept SSLVPN connections (Enterprise, in this case)
- Certificate that has to be accepted by the enterprise user

- Connection group alias/URL. Refer to Figure 4-24.

Figure 4-24 Cisco SSLVPN Connection Profile Configuration

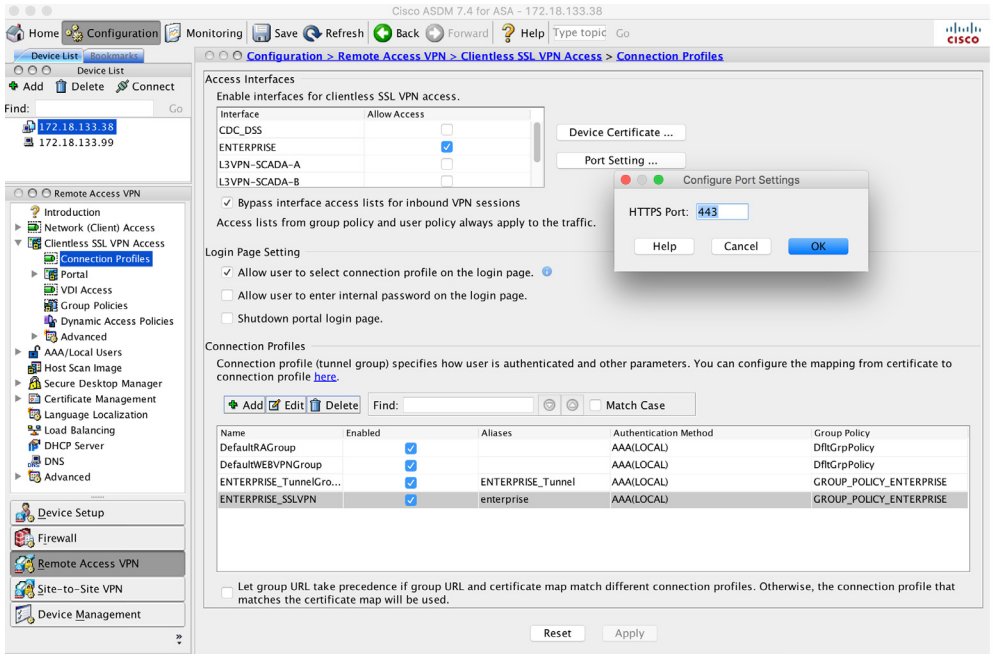


Navigate the wizard to select the **Group Policy**, **Allowed Users,** and **Bookmark** lists.

Step 2 Ensure that the group policy, users, authentication information are correctly applied to the interface facing the enterprise. Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

Ensure that the port setting (port number 443) for the HTTP secure access is correctly selected. Allow the enterprise user to select the previously configured connection profile. Ensure the authentication used is local. Apply the configuration. Refer to Figure 4-25.

Figure 4-25 Cisco SSLVPN Connection Profile Application



The equivalent configuration for Steps 1-2 is shown below:

```
!
name 192.168.140.0 ENTERPRISE description ENTERPRISE
ip local pool ENTERPRISE_POOL 209.165.200.1-209.165.200.50 mask 255.255.255.0
!
!
interface Port-channel3.140
 vlan 140
 nameif ENTERPRISE
 security-level 50
 ip address 192.168.140.1 255.255.255.0 standby 192.168.140.2
!
access-list 140 extended permit ip 192.168.140.0 255.255.255.0 192.168.125.0
255.255.255.0
access-list 140 extended permit ip 209.165.200.0 255.255.255.0 192.168.125.0
255.255.255.0
!
access-group 140 in interface ENTERPRISE
!
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ASDM_TrustPoint0 ENTERPRISE
!
webvpn
 enable ENTERPRISE
 anyconnect image disk0:/anyconnect-macosx-i386-2.5.2014-k9.pkg 1
 anyconnect image disk0:/anyconnect-linux-2.5.2014-k9.pkg 2
 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 3
 anyconnect profiles CLIENT_PROFILE_ENTERPRISE disk0:/client_profile_enterprise.xml
 anyconnect enable
 tunnel-group-list enable
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
group-policy GROUP_POLICY_ENTERPRISE internal
group-policy GROUP_POLICY_ENTERPRISE attributes
```

```
 banner value Welcome ENTERPRISE user !!
 wins-server none
 dns-server value 64.102.6.247
 vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 default-domain value cisco.com
 address-pools value ENTERPRISE_POOL
 webvpn
  url-list value CLIENTLESS_SSLVPN_BOOKMARK_LIST
  anyconnect profiles value CLIENT_PROFILE_ENTERPRISE type user
  always-on-vpn profile-setting
username admin password 5oxw0ynT1T/GuVUW encrypted privilege 15
username enterprise1 password Fs8gBKi97OcGuaV3 encrypted privilege 15
username enterprisessl password XzyTDmDHO3fE8aUe encrypted privilege 15
       username enterprisessl attributes
        vpn-group-policy GROUP_POLICY_ENTERPRISE
       tunnel-group ENTERPRISE_SSLVPN type remote-access
       tunnel-group ENTERPRISE_SSLVPN general-attributes
        default-group-policy GROUP_POLICY_ENTERPRISE
       tunnel-group ENTERPRISE_SSLVPN webvpn-attributes
        group-alias enterprise enable
        group-url https://192.168.140.1/enterprise enable
!
```

Cisco AnyConnect VPN

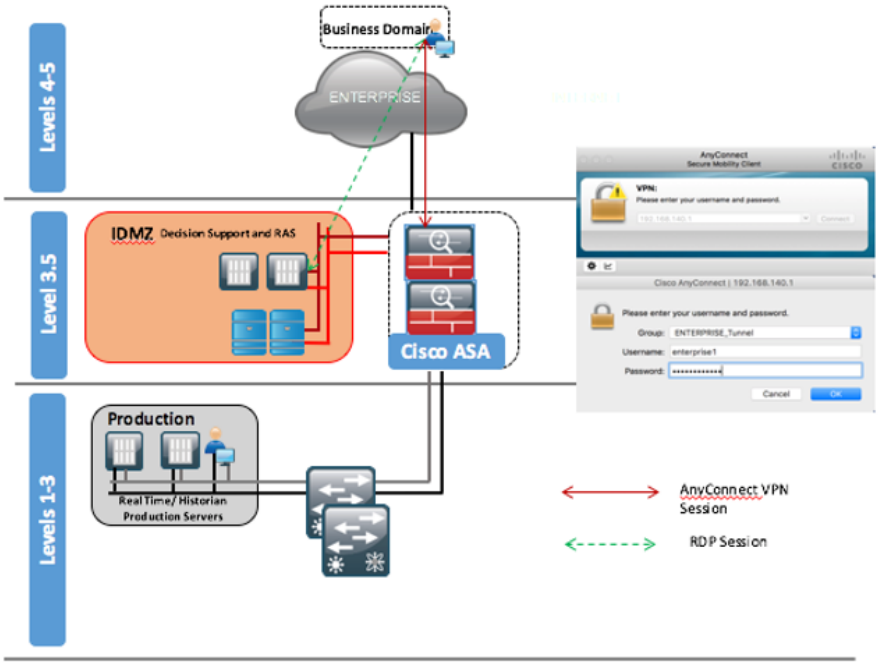
The firewall is set up with Cisco AnyConnect, which enables the end user to download the remote access client for VPN connectivity to the DSS zone.

This scenario is specifically mentioned for a user located inside enterprise network. The user will make use of a Cisco AnyConnect VPN client installed on his computer to directly access servers in DSS zone. Once the VPN session is authenticated, the user will be able to access servers in DSS zone via RDP. Refer to Figure 4-26.

Necessary ports are opened on the firewall for the enterprise user to communicate with servers in the DSS zone.

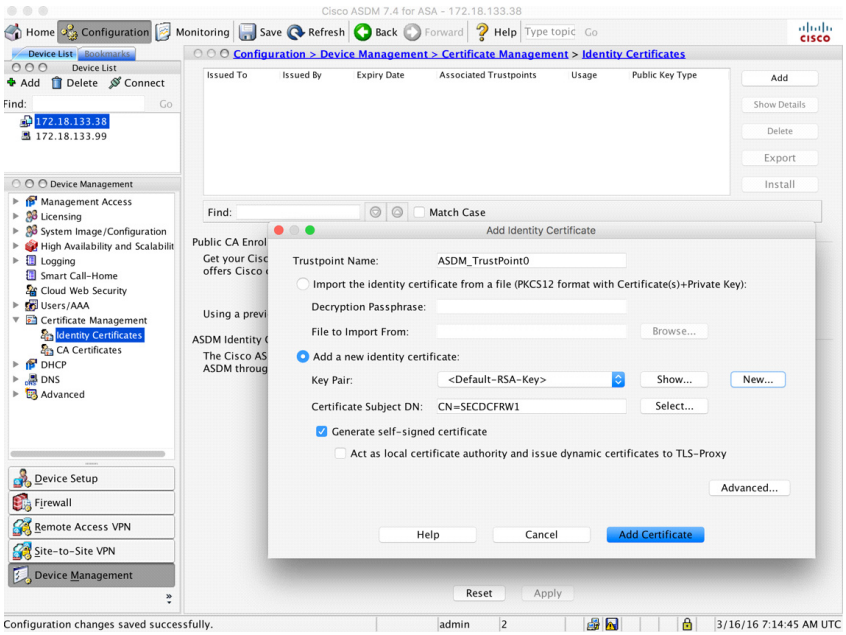
Note This scenario is strictly for a user within the corporate network as multiple AnyConnect sessions cannot exist at any given point in time.

Figure 4-26 Remote Access using Cisco AnyConnect (Enterprise User)



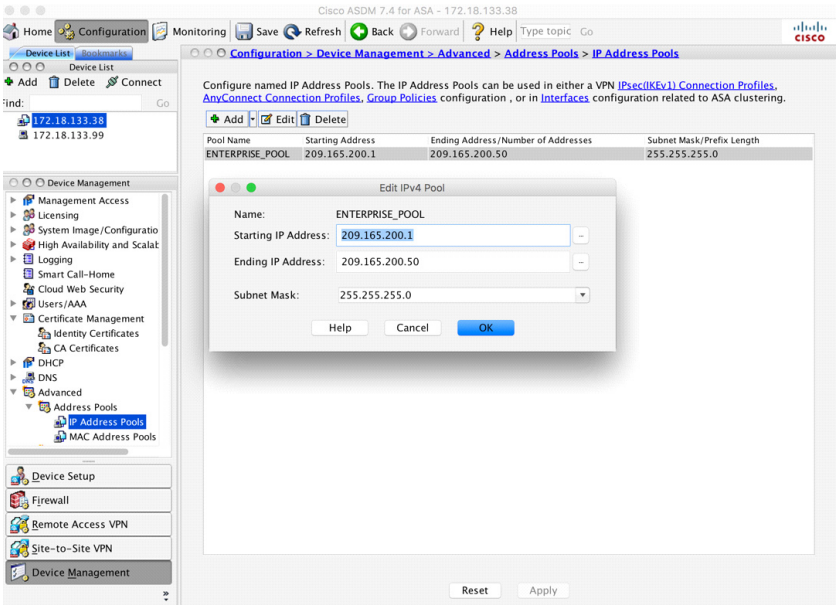
Step 1 Configure the ASA5525x to generate a self-signed certificate for all incoming sessions using ASDM. Navigate to **Configuration > Device Management > Certificate Management > Identify Certificates**. Add a new identity certificates. Refer to Figure 4-27.

Figure 4-27 Identity Certificate Management for Enterprise



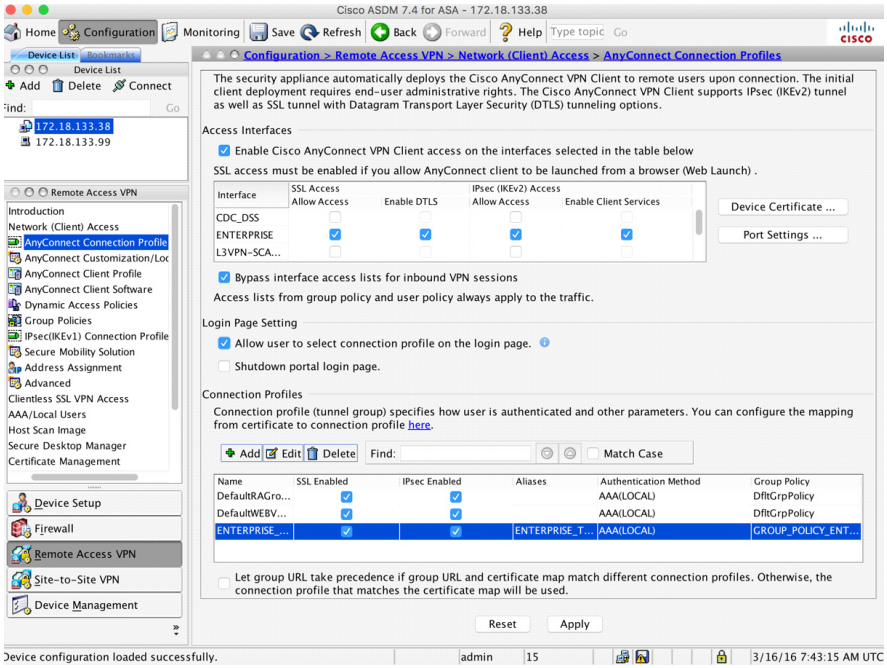
Step 2 Configure an address pool for the enterprise users. Any enterprise user logging into DSS zone will be assigned an IP address from this pool during the secure connection session. In ASDM, navigate to **Configuration > Device Management > Advanced > Address Pools > IP Address Pools**. Add a new entry and reserve a pool of IP addresses. For this implementation, an IP address in the range of 209.165.200.1 - 50 were allocated. Refer to Figure 4-30.

Figure 4-28 Address Pool for Enterprise Users



Step 3 Configure AnyConnect connection profile in the ASDM for remote access VPN. Enable the interface towards Enterprise for SSL access and assign connection profiles. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** and enable. Refer to Figure 4-29 for steps.

Figure 4-29 AnyConnect Connection Profile for Remote Access VPN



The equivalent CLI configuration for Steps 1-3 is shown below:

```
!
name 192.168.140.0 ENTERPRISE description ENTERPRISE
ip local pool ENTERPRISE_POOL 209.165.200.1-209.165.200.50 mask 255.255.255.0
!
!
interface Port-channel3.140
 vlan 140
 nameif ENTERPRISE
 security-level 50
 ip address 192.168.140.1 255.255.255.0 standby 192.168.140.2
!
access-list 140 extended permit ip 192.168.140.0 255.255.255.0 192.168.125.0
255.255.255.0
access-list 140 extended permit ip 209.165.200.0 255.255.255.0 192.168.125.0
255.255.255.0
!
access-group 140 in interface ENTERPRISE
!
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ASDM_TrustPoint0 ENTERPRISE
!
webvpn
 enable ENTERPRISE
 anyconnect image disk0:/anyconnect-macosx-i386-2.5.2014-k9.pkg 1
 anyconnect image disk0:/anyconnect-linux-2.5.2014-k9.pkg 2
 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 3
 anyconnect profiles CLIENT_PROFILE_ENTERPRISE disk0:/client_profile_enterprise.xml
 anyconnect enable
 tunnel-group-list enable
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
group-policy GROUP_POLICY_ENTERPRISE internal
group-policy GROUP_POLICY_ENTERPRISE attributes
 banner value Welcome ENTERPRISE user !!
 wins-server none
```

```
 dns-server value 64.102.6.247
 vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 default-domain value cisco.com
 address-pools value ENTERPRISE_POOL
 webvpn
  anyconnect profiles value CLIENT_PROFILE_ENTERPRISE type user
  always-on-vpn profile-setting
username admin password 5oxw0ynT1T/GuVUW encrypted privilege 15
username enterprise1 password Fs8gBKi97OcGuaV3 encrypted privilege 15
tunnel-group ENTERPRISE_TunnelGroup1 type remote-access
tunnel-group ENTERPRISE_TunnelGroup1 general-attributes
 address-pool ENTERPRISE_POOL
 default-group-policy GROUP_POLICY_ENTERPRISE
tunnel-group ENTERPRISE_TunnelGroup1 webvpn-attributes
 group-alias ENTERPRISE_Tunnel enable
 group-url https://192.168.140.1/ENTERPRISE_Tunnel enable
!
```

Network Infrastructure Security Implementation

An extra level of security within the Control Center switching infrastructure is provided in the categories described in this section.

Shutdown Unused Ports

Any unused port on the Nexus 3524 switch is explicitly placed in administratively shutdown mode.

```
!
interface Ethernet1/10
  description UNUNSED PORT
  shutdown
!
Nx3548-SECDCSW1# show interface Ethernet 1/10
Ethernet1/10 is down (SFP not inserted)
 Dedicated Interface
  Hardware: 100/1000/10000 Ethernet, address: 5897.bd73.abd1 (bia 5897.bd73.abd1
)
  Description: UNUNSED PORT
>> snip <<
```

Trunk Ports

In the current implementation, trunk ports on Nexus 3524 switches are configured for explicit trunk with Dynamic Trunk Protocol (DTP) off. Only necessary VLANs are allowed on the trunks.

```
!
interface Ethernet1/3
  speed 1000
  description TO_SECDCFRW1::Gig0/3
  switchport mode trunk
  switchport trunk allowed vlan 120,122,125
  channel-group 3 mode active
  no shutdown
!
interface port-channel3
  description PORTCHANNEL_TO_SECDCFRW
  switchport mode trunk
  switchport trunk allowed vlan 120,122,125
```

```
  vpc 3
!
```

Port Security

Port Security is configured to limit unauthorized use of a switch ports. This feature is usually enabled on access ports connected to operator stations. Generally, the work stations will physically be in a different location so the Control Center VLAN must be extended from the Nexus 3524 switch to an enterprise access switch such as Catalyst 3850.

In the following example, an access port on a Catalyst 3850 switch connected to an operator station is configured for port-security.

```
!
interface GigabitEthernet1/0/21
  description PRODUCTION_OPERATOR_STATION_1
  switchport access vlan 120
  switchport port-security violation restrict
  switchport port-security mac-address sticky
  switchport port-security
  switchport port-security mac-address AABB.CCDD.EEFF

!

3850-ACCESS#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------
   Gi1/0/21              1            1                  0         Restrict
--------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
3850-ACCESS#


3850-ACCESS#sh port-security interface gigabitethernet 1/0/21
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : ac87.a323.cff2:201
Security Violation Count   : 33

3850-ACCESS#
```

Storm Control

No formal requirement for the storm control feature for BLISS Control Center virtualization implementation exists. However, to showcase the feature, storm control is configured on port-channel interfaces to limit the broadcast storm to 75% of the available bandwidth.

Example:

```
!
interface port-channel3
```

```
  description PORTCHANNEL_TO_SECDCFRW
  switchport mode trunk
  switchport trunk allowed vlan 120,122-123,125
  storm-control broadcast level 75.00
  vpc 3
!

Nx3548-SECDCSW1# sh interface port-channel 3 counter storm-control
--------------------------------------------------------------------------------
Port        UcastSupp %  McastSupp %  BcastSupp %  TotalSuppDiscards
--------------------------------------------------------------------------------
Po3              100.00       100.00        75.00                  0
Nx3548-SECDCSW1#
```

Infrastructure Management

In the current implementation, out-of-band (OOB) management is deployed for the management of network infrastructure. A dedicated VLAN 10 with IP address range of *10.27.x.x/16* is used within the lab infrastructure. Secure shell (SSH), a cryptographic network protocol provides a secure channel for connecting to the networking infrastructure.

```
!
aaa new-model
ip domain name schneider-electric.com
!
!
username testuser password 0 testpassword
!
ip ssh time-out 60
ip ssh version 1
!
line vty 0 4
 exec-timeout 0 0
 password lab
 logging synchronous
 transport preferred none
 transport input ssh
!

SECDCRTR2#telnet 10.27.3.8 /vrf Mgmt-intf
Trying 10.27.3.8 ...
% Connection refused by remote host

SECDCRTR2#
SECDCRTR2#ssh -l testuser -vrf Mgmt-intf 10.27.3.8
Password:

SECDCRTR1>
```

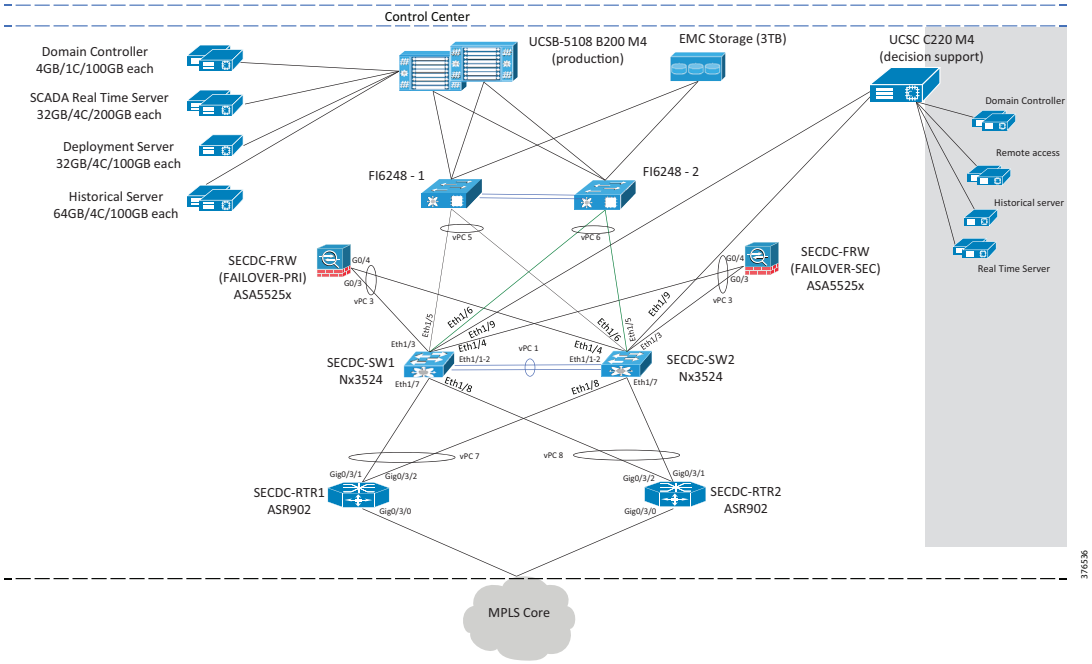
High Availability Implementation

One of the primary requirements of a Control Center environment is to provide high availability to ensure seamless operation in case of a failure to any portion of the infrastructure. The Control Center infrastructure is validated for high availability in the following categories.

Network Redundancy

Figure 4-30 provides an overview of different equipment implemented in a highly available infrastructure in alignment with the design of the Control Center.

Figure 4-30 Control Center Infrastructure



Port-Channel

Multiple physical links connecting two devices are included to be part of a port-channel to create one logical link. Such a logical link aggregates bandwidth and provides redundancy in case one of the links in the bundle fails. Traffic on the failed link is carried over to the remaining individual links between the devices.

Physical links connecting WAN edge routers and Nexus 3524 switches are bundled into port-channel.

```
!
interface GigabitEthernet0/3/1
 description TO_SECDCSWT::Gig2/0/1
 channel-group 2 mode active
!
interface GigabitEthernet0/3/2
 description TO_SECDCSWT::Gig1/0/1
 channel-group 2 mode active
!
!
interface Port-channel2
 ip vrf forwarding SCADA_A
 ip address 192.168.122.4 255.255.255.0
 vrrp 120 ip 192.168.122.1
 vrrp 120 priority 110
 vrrp 120 preempt
!
```

Similarly, physical links connecting ASA5525x firewall and Nexus 3524 switches are bundled into port-channel.

```
!
interface GigabitEthernet0/3
 description TO_SECDCSWT::Gig1/0/3
 channel-group 3 mode active
!
interface GigabitEthernet0/4
 description TO_SECDCSWT::Gig2/0/4
 channel-group 3 mode active
!
!
interface Port-channel3
 lacp max-bundle 8
 no nameif
 no security-level
 no ip address
!
```

Virtual Port-Channel (vPC)

The two Nexus 3524 switches are made to behave like a single logical entity to other attached devices like WAN edge routers, Fabric Interconnects, and the firewall. This is accomplished by having a vPC peer link between the two switches.

A vPC allows multiple physical links to be bundled into a port-channel and pair with other port-channel-enabled devices providing link level redundancy.

Figure 4-30 indicated different vPCs configured on the Nexus switches and the VLANs allowed on each vPC.

vPC 1 is configured to be the peer-link and is responsible for carrying both vPC and non-vPC VLAN information. vPC peers must synchronize the Layer 2 forwarding table: that is, the MAC address information between the vPC peers. This way, if one vPC peer learns a new MAC address, that MAC address is also programmed on the Layer 2 forwarding table of the other peer device

An example configuration of one such vPC is shown here:

```
!
interface Ethernet1/7
  speed 1000
  description TO_SECDCRTR1::Gig0/3/1
  switchport access vlan 122
  channel-group 7 mode active
  no shutdown
!
interface port-channel7
  description PORTCHANNEL_TO_SECDCRTR
  switchport access vlan 122
  vpc 7
!
```

ASA Redundancy

The Cisco ASA platform is deployed in the Control Center to provide firewall capability. A pair of ASA 5525-X platforms are set up in an active/standby mode for high availability. Both these firewalls are connected to the Nexus switch assembly as shown in the topology. A failover link is configured between

the two ASA 5525-Xs to determine the primary and secondary roles. The failover link is a directly-attached link between the two ASA 5525-Xs in the BLISS setup. Alternately, this link can be set up via an external switch.

Configure active/standby failover mode on each firewall and the failover link between the two (refer to Figure 4-31, Figure 4-32, and Figure 4-33).

Step 1 Select **High Availability and Scalability > Failover** within the Device Management pane.

Step 2 In the **Setup** tab, select **Enable Failover**. For greater security, enter a shared key in the appropriate field to encrypt the communications between the active and standby firewalls.

Step 3 Under **LAN Failover**, select a physical interface to transmit failover information. Fill in the **Logical Name** field with any desired value, as well as the **Active IP** and **Standby IP** fields (select any IP address range not already being used) and the Subnet Mask field (typically *255.255.255.252* for a point-to-point connection).

Step 4 Select the **Preferred Role** to identify whether this firewall should be the primary (active) or secondary (standby). Under **State Failover**, select a physical interface (may be the same as LAN Failover interface, if desired).

Step 5 In the **Interfaces** tab, assign a standby IP address for each interface within the same subnet as the active one. For any interfaces that should be monitored for loss of connectivity to trigger a firewall failover, select the **Monitored** option.

Step 6 In the **Criteria** tab, enter **1** as the **Number of failed interfaces that triggers failover**. Change values under **Failover Poll Times** as desired.

Step 7 Click **Apply** to make all changes take effect.

Step 8 Repeat the above process for the second firewall (changing the **Preferred Role** accordingly).

Note When Stateful Failover is enabled, the active unit continually passes per-connection state information to the standby unit via the State Failover link.

Figure 4-31 ASA 5525-X Failover Configuration-1

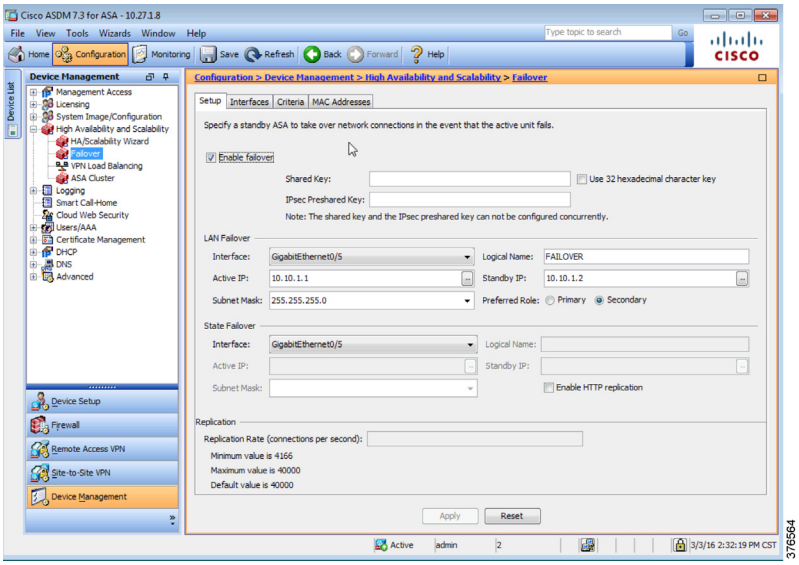


Figure 4-32 ASA 5525-X Failover Configuration-2

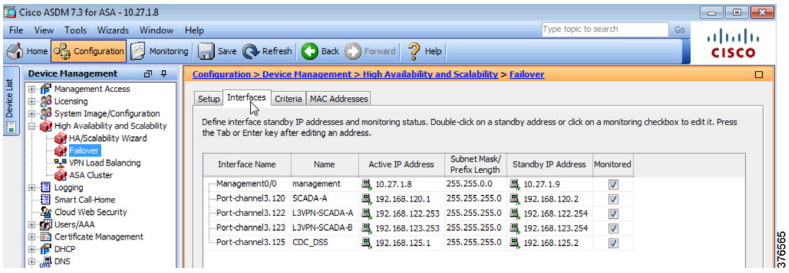
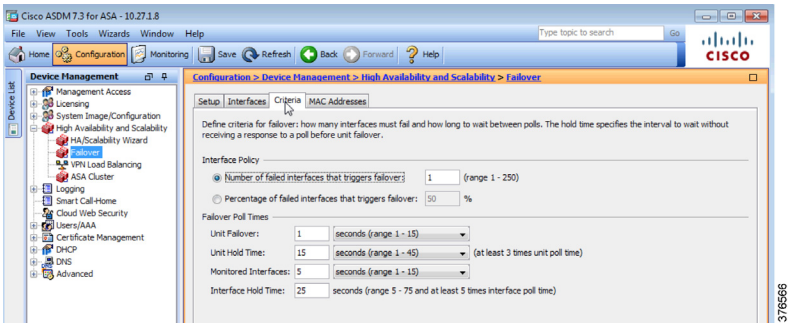


Figure 4-33 ASA 5525-X Failover Configuration-3



The equivalent CLI configuration for ASA failover is shown below:

```
!
failover
failover lan unit primary
failover lan interface FAILOVER GigabitEthernet0/5
failover link FAILOVER GigabitEthernet0/5
failover interface ip FAILOVER 10.10.1.1 255.255.255.0 standby 10.10.1.2
!
monitor-interface SCADA-A
```

```
monitor-interface L3VPN-SCADA-A
monitor-interface CDC_DSS
!
```

On the redundant ASA equipment, the CLI equivalent will be:

```
!
failover
failover lan unit secondary
failover lan interface FAILOVER GigabitEthernet0/5
failover link FAILOVER GigabitEthernet0/5
failover interface ip FAILOVER 10.10.1.1 255.255.255.0 standby 10.10.1.2
!
monitor-interface SCADA-A
monitor-interface L3VPN-SCADA-A
monitor-interface CDC_DSS
!
```

Edge Router Redundancy

The edge router is not part of the BLISS design; however, they help Control Center communicate with the Pipeline Network segment. Two ASR edge routers are deployed within the Control Center to provide redundant connection to the WAN. These edge routers peer with the Nexus 3524 via port-channel. They also peer with a Multiprotocol Label Switching (MPLS)-enabled core router for receiving network layer information from the Pipeline.

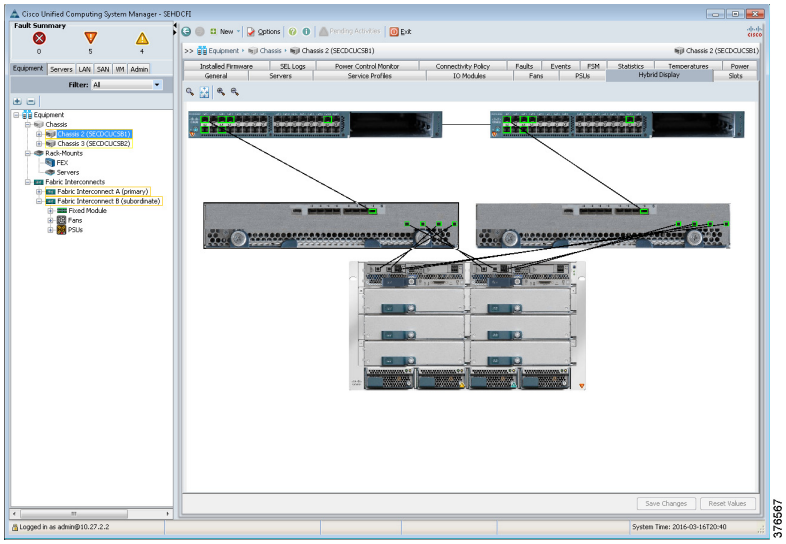
Compute Redundancy

This section describes Compute redundancy implementation.

Fabric Redundancy

An equal number of connections are made from the Fabric Interconnect server ports to the backplane of the UCS chassis. This allows the vNICs and vHBAs provisioned to the blade servers to have multiple paths from the chassis out into the Data Center. While traffic will flow through the Fabric Interconnect associated with the vNIC, failover can be enabled to utilize the additional Fabric Interconnect in the case of a failure. This also removes the need to configure NIC Teaming on the Hyper-V server, as the path redundancy is now handled by the Fabric Interconnects (see Figure 4-34).

Figure 4-34 Fabric Redundancy in Control Center



End Host Mode

This is the default configuration on the Fabric Interconnects and is recommended in this architecture since they are connected to an upstream switch.

End-host mode features include the following:

- STP is not run on both the uplink ports and the server ports.
- MAC address learning occurs only on the server ports; MAC address movement is fully supported.
- Links are active/active regardless of the number of uplink switches.
- The system is highly scalable because the control plane is not occupied.

More details related to Fabric redundancy and end host mode can be found at *Cisco Unified Computing System Ethernet Switching Modes* at the following URL:

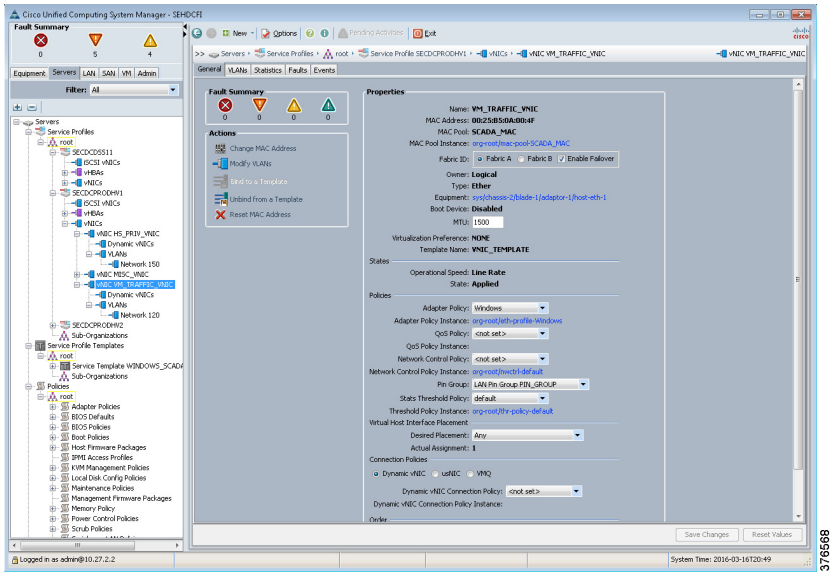
- http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/whitepaper_c11-701962.html

SCADA Server Connectivity and Redundancy (Virtual Machines)

In the Production environment, two B series servers will exist. Each of these servers will be running duplicate virtual machines for each service. In addition, the two B series servers will reside on physically separate chassis. This way if there is any hardware failure between the chassis or the actual blade, the corresponding duplicate virtual machine will take over.

In addition to hardware redundancy, the B series servers will have network redundancy to the Fabric Interconnects. Traditionally this would be done by allocating two NICs to the B series servers and configuring a NIC team. However, only one NIC is needed for virtual machine traffic since redundant connectivity to the Fabric Interconnects is performed via Fabric Failover (see Figure 4-35).

Figure 4-35 NIC Failover Enabled



In Hyper-V, the virtual switch is mapped to this NIC, thereby giving the same network redundancy to any virtual machines using the virtual switch (as seen in the Compute Segmentation section).

Storage Redundancy

The storage redundancy is built into the storage segmentation. Multiple VSANs, in addition to two HBAs per B series server, allow for redundant paths to the external storage.

Application Redundancy

This section describes application redundancy application.

VM Redundancy

In the Production zone, one set of servers, namely RealTime, Historical, Domain Controller, and Logging, are deployed for each application. These servers are housed on a redundant UCS B 5108 infrastructure having B200 M4 blade servers. For example, the hot version of the RealTime server resides on Blade1/Chassis1 and the standby version of the same application resides on Blade1/Chassis2. The redundancy mechanism built into OASyS software and applications decides which instance is chosen as hot/standby.

Operator Workstation Connectivity

In the current implementation, operator workstations are located in the same facility as the Control Center infrastructure. These operator stations are connected to Nexus 3524 switch ports. These switch ports are configured as access ports and unused ports on the switch are shutdown.

```
!
interface Ethernet1/32
description PRODUCTION_OPERATOR_STATION_1
switchport access vlan 120
```

```
    !
    !
    interface Ethernet1/46
    description UNUSED_PORT
     shutdown
!
```

Note In case of operator stations located at a different location, the LAN segment has to be extended. In such situation, an Enterprise Catalyst switch such as 3850 is used to connect operator stations. Necessary security measures like port security are deployed for such ports.

```
    !
    interface Ethernet1/32
      description PRODUCTION_OPERATOR_STATION_1
      switchport access vlan 120
      switchport port-security violation restrict
      switchport port-security mac-address sticky
      switchport port-security
      switchport port-security mac-address AABB.CCDD.EEFF

    !
```

Network Management and Time Synchronization

This section describes implementation for network management and time synchronization.

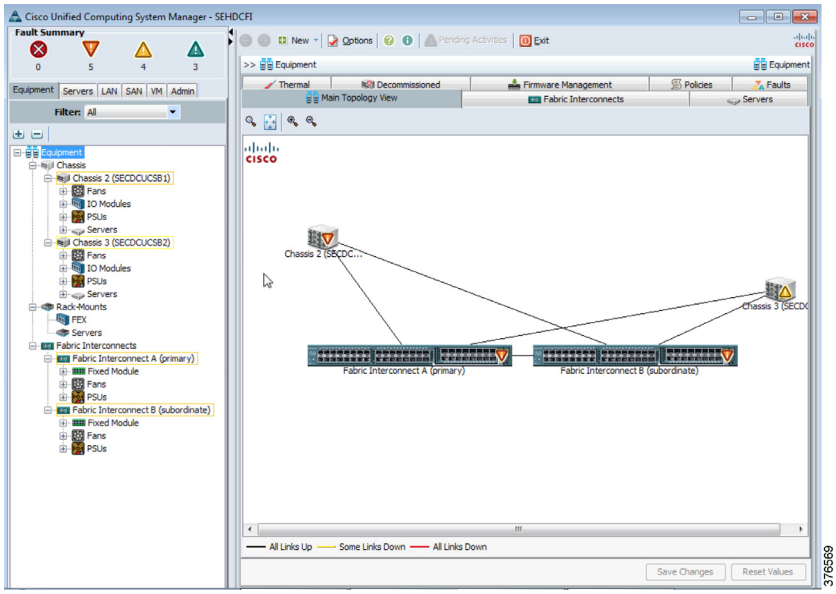
Network Management

In the current implementation of Control Center virtualization, network management of the Control Center equipment is spread across using multiple tools, which are described in this section.

UCS Manager

The Production zone application servers are hosted on B200 M4 blade servers on a redundant UCSB 5108 chassis. This setup is managed by accessing the UCS Fabric Interconnects. UCS Manager resides on the Fabric Interconnects and provides a management environment for the Production zone. UCS Manager is accessed via HTML. Figure 4-36 provides a representation of accessing the Production zone via UCS manager for managing application servers.

Figure 4-36 UCS Manager



Cisco Integrated Management Controller

The DSS zone application servers are hosted on a C220 M4 rack mount server. This setup is managed by accessing the Cisco Integrated Management Controller (CIMC) via HTML. Figure 4-37 and Figure 4-38 represent accessing the DSS zone via CIMC and launching a Kernel-based Virtual Machine (KVM) console for managing application servers.

Figure 4-37 Cisco Integrated Management Controller

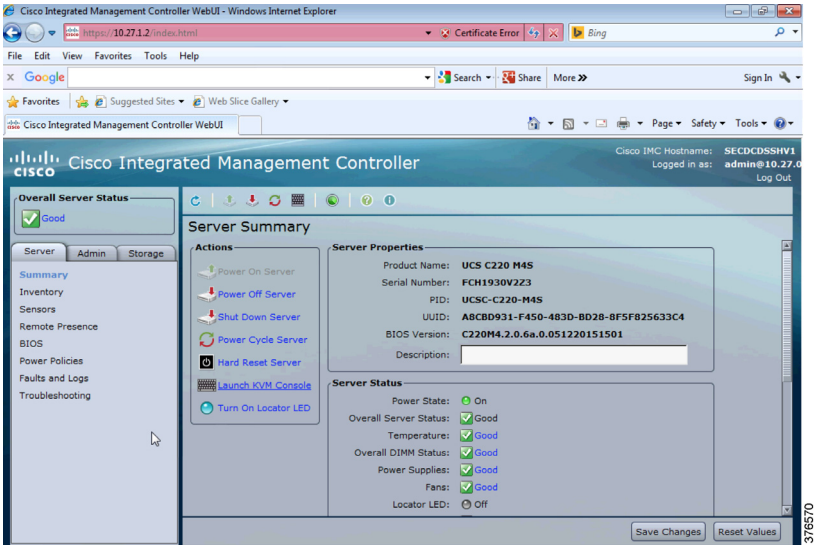
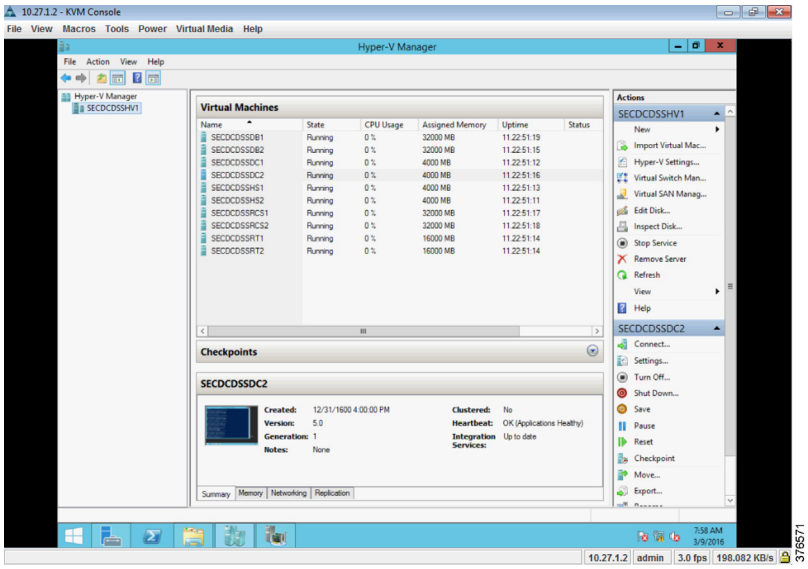


Figure 4-38 KVM Console for Management



SNMP and Logging Server

Simple Network Management Protocol (SNMP) network management is implemented on the network equipment within the Control Center. The SNMP manager is located within the Control Center in the Production zone. All the equipment is configured to send traps to this SNMP manager.

```
!
snmp-server group STRUXURELAB v3 auth
snmp-server user lab STRUXURELAB v3 encrypted auth md5
36:e3:70:34:95:8e:ce:00:3a:80:73:e4:7f:dc:cd:a4
snmp-server host SCADA-A 192.168.120.91 trap version 3 lab
snmp-server location CDC
snmp-server contact struxurelab@schneider-electric.com
snmp-server community *****
!
```

The SNMP Manager host machine also acts as the logging server located within the Control Center. Network equipment are configured to send logs to this logging host.

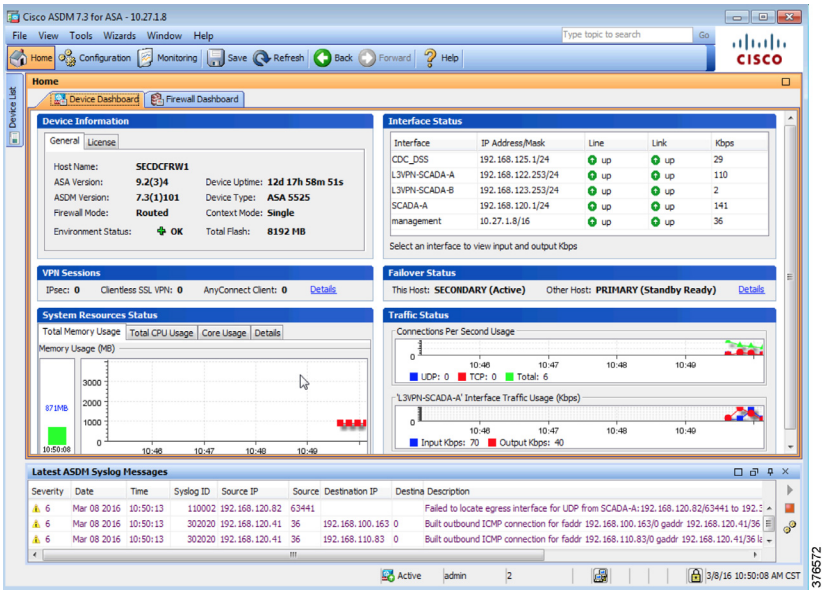
```
!
logging enable
logging timestamp
logging buffer-size 1048576
logging buffered debugging
logging asdm informational
logging host SCADA-A 192.168.120.91
!
```

Cisco Adaptive Security Device Manager

The ASA 5525-X within the Control Center that is used as a firewall is managed by using Adaptive Security Device Manager (ASDM). The ASDM user interface (see Figure 4-39) provide easy access to configure the interface, routing, firewall policy, and general management of the firewall. ASDM version 7.3 was used in the implementation to manage ASA 5525-X with image version 9.2.

Note ASDM supports many ASA versions. ASDM documentation and online help includes all of the latest features supported by the ASA.

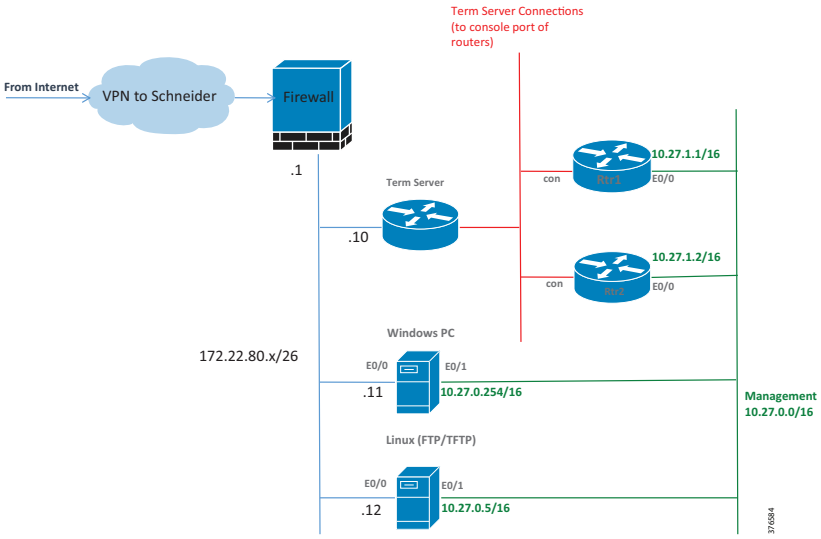
Figure 4-39 ASDM User Interface



Out of Band Management

In the current implementation of Control Center virtualization, OOB management network is deployed to provide dedicated management of the infrastructure. Refer to Figure 4-40 for a representative network for OOB management.

Figure 4-40 Out of Band Management



VLAN 10 is the dedicated VLAN used for this OOB management. The functionality of this OOB management includes the following:

- Console access to any networking equipment such as Nexus 3524 switches, ASA firewall, and ASR WAN edge routers
- FTP/TFTP servers for any file transfer
- UCS Manager for blade servers
- CIMC for rack mount servers

Time Synchronization

In the current implementation of Control Center virtualization, a time source is set up in the Control Center Production zone. The clock source is configured to propagate the accurate time information with a Stratum level 4. Networking equipment within the Control Center and Pipeline stations are configured to reference this time source for synchronization.

Note For the lab setup, Stratum 4 was configured.

NTP Source:

```
!
interface GigabitEthernet0/0/0
 ip address 192.168.120.177 255.255.255.0
 ntp broadcast
!
ntp master 4
!

NTP-SERVER#sh ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~127.127.1.1     .LOCL.           3      9     16   377  0.000   0.000  1.204
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

NTP-SERVER #sh ntp status
Clock is synchronized, stratum 4, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 8731900 (1/100 of seconds), resolution is 4000
reference time is DA8315F8.6353F8E0 (13:58:48.388 CST Thu Mar 3 2016)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.18 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 0 sec ago.
NTP-SERVER #sh clock
13:58:50.420 CST Thu Mar 3 2016
```

Other equipment (shown here is an example configuration on the firewall within Control Center):

```
!
ntp server 192.168.120.177 prefer
!

SECDCFRW1# sh ntp associations
      address         ref clock     st  when  poll reach  delay  offset    disp
*~192.168.120.177  127.127.1.1       4    29   128  377     0.3    0.80    16.1
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
SECDCFRW1#
```

```
SECDCFRW1# sh ntp status
Clock is synchronized, stratum 5, reference is 192.168.120.177
nominal freq is 99.9984 Hz, actual freq is 100.0082 Hz, precision is 2**6
reference time is da8315aa.cfcdb998 (13:57:30.811 CST Thu Mar 3 2016)
clock offset is 0.4077 msec, root delay is 0.27 msec
root dispersion is 18.48 msec, peer dispersion is 15.88 msec
SECDCFRW1# sh clock
13:58:36.745 CST Thu Mar 3 2016
!
```

Control Center Virtualization: Validation

Functionality, high availability, and security testing were performed as part of the Control Center virtualization validation. Detailed information on various options can be found in the *Control Center Virtualization for the Connected Pipeline System Design Guide*. This chapter includes the following major topics:

Functionality Testing

Functional testing was validated once the control system operation was up and running. The aggregation routers were able to reach the Pipeline Network through the configured VRF instance. SCADA application servers in both the Production and DSS zones could reach their respective default gateways on the firewall assembly. The SCADA application servers in the Production zone of the Control Center were polling/monitoring information from the Pipeline PLCs. This data was replicated to servers in the DSS zone. SCADA application servers in the DSS zone were denied access for the Pipeline Network. Policy set on the firewall controlled the access between Control Center and Pipeline Network. Access switches in the Control Center provided communication path for the UCS, firewall, storage array, and aggregation routers.

High Availability Testing

A set of SCADA servers for each application (RealTime, Domain Controller, and Historical) were provisioned in both the Production and DSS zones. Communication at the application level decides which server is active/standby. Redundancy is provisioned at every level of the Control Center - SCADA servers, UCS chassis, SCADA servers on different blades (active on blade 1 chassis 1; standby on blade1 chassis 2), a pair of firewalls (primary/secondary), a pair of access switches, and a pair of aggregation routers.

The system was validated for high availability in all of the following scenarios:

- **Failure**—Physical link, port-channel, node, line card, firewall, power, Fabric Interconnect-to-IO module port disable
- **Reload**—Aggregation router, access switch, SCADA application server, blade server, primary and secondary, virtual switch, Fabric Interconnect, and UCS-B chassis reboot

In the case of a network failure, the active server instance ceased to monitor the Pipeline Network for 3-5 seconds until re-convergence of the system via alternate path.

In the case of a SCADA active server failure, the downtime was observed to be 10-15 seconds before the standby server took control.

Security Testing

Security testing was completed and verified routing instances on the aggregation routers, firewall policies, and vPC tables and allowed VLANs in the Nexus switches. The Pipeline Network was seen in the appropriate VRF instance on the aggregation routers. This information was redistributed internally in the Control Center to firewall. The firewall policy definition provided access only between the Production zone and the Pipeline Network. It was ensured there was no direct access from the DSS zone to Pipeline Network. Only necessary VLANs for Production, DSS and L3VPN were configured on the nexus switch. All the unused ports on the Nexus switches were configured for port security shutdown mode.

Control Center Virtualization: Verification

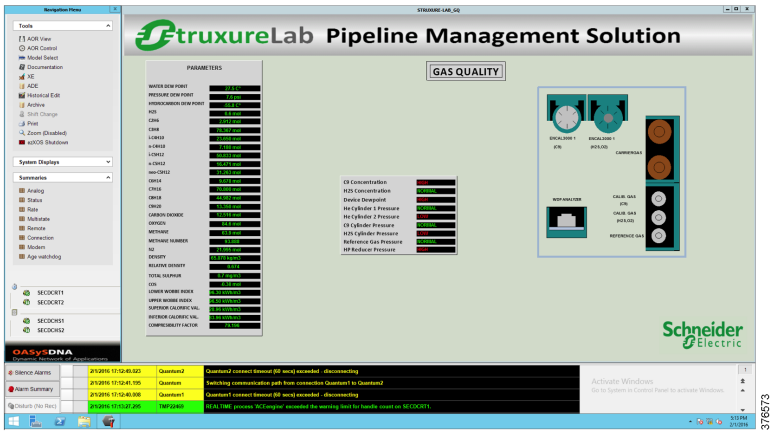
This Appendix, which describes verification of Control Center virtualization from functional, security, and redundancy standpoints, includes the following major topics:

Functional Verification—Control Center RealTime Application Gathering Field Data

This section outlines verification of communication between Control Center equipment and field devices such as PLCs. Some of the verification includes route table lookup in edge routers, firewall/gateway route lookup, and application servers receiving data from field devices.

Figure A-1 shows the RealTime application server monitoring field device.

Figure A-1 Verification: Production RealTime Server Polling PLCs in Pipeline Station



Both the Pipeline Network segment 192.168.100.0/24 and Production zone network 192.168.120.0/24 can be seen in the route table of the edge router in the following CLI output:

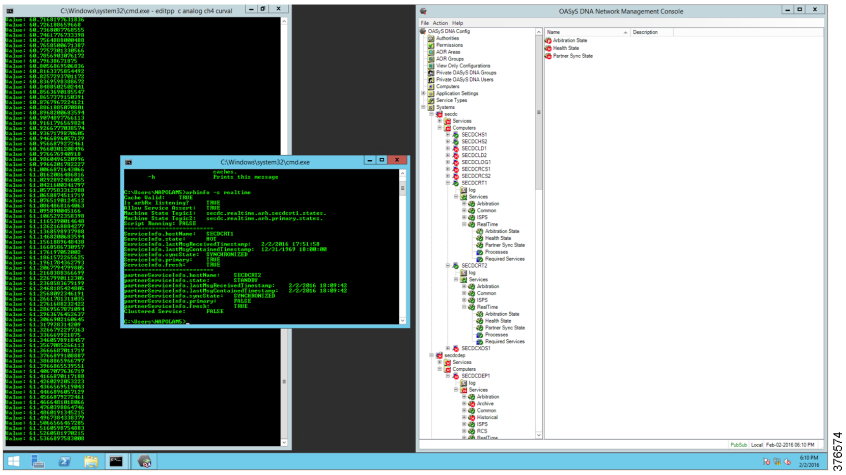
```
SECDCRTR1#show ip route vrf SCADA_A
```

```
Routing Table: SCADA_A
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

D*    0.0.0.0/0 is a summary, 3w0d, Null0
B     192.168.4.0/24 [200/0] via 192.168.1.1, 3w0d
B     192.168.100.0/24 [200/100] via 192.168.1.1, 3w0d
D     192.168.120.0/24 [90/3072] via 192.168.122.253, 3w0d, Port-channel2
      192.168.122.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.122.0/24 is directly connected, Port-channel2
L        192.168.122.4/32 is directly connected, Port-channel2
D     192.168.125.0/24 [90/3072] via 192.168.122.253, 3w0d, Port-channel2
SECDCRTR1#

Ping from Router to PLC successful:

SECDCRTR1#ping vrf SCADA_A 192.168.100.163
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.163, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/16/40 ms
SECDCRTR1#
```

Redundancy Verification—SCADA Application Server Reload

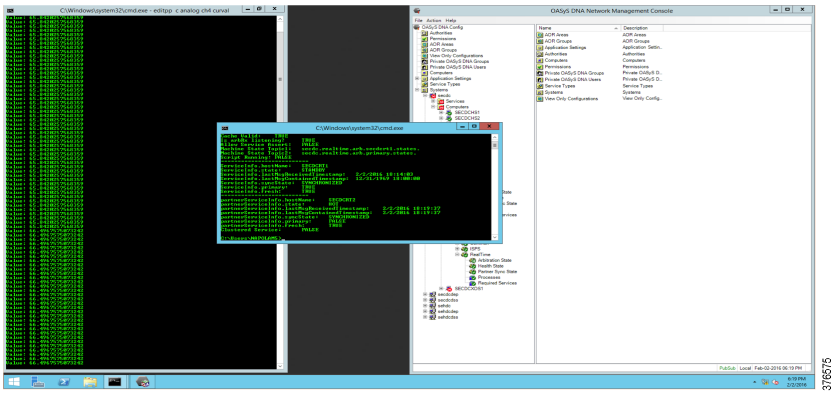
With the system stable, SECDCRT1 is the hot RealTime server and SECDCRT2 is the standby RealTime server (see Figure A-2).

Figure A-2 Verification: RealTime Server—1 is HOT Before Reload



Resetting the hot RealTime server triggers communication failure between the hot/standby servers. The standby (SECDCRT2) polls for three timeout periods (5 x 3 seconds) and assumes the role of active server. When SECDCRT1 reboots, it assumes the role of standby server (see Figure A-3).

Figure A-3 Verification: RealTime Server—1 is STANDBY After Reload



ASA/Firewall Failover

The following output shows the many options available to verify the ASA failover states:

```
SECDCFRW1# show failover ?
```

Descriptor	Show failover interface descriptors. Two numbers are shown for each interface. When exchanging information regarding a particular interface, this unit uses the first number in messages it sends to its peer. And it expects the second number in messages it receives from its peer. For troubleshooting, collect the show output from both units and verify that the numbers match.
Exec	Show failover command execution information
History	Show failover switching history
Interface	Show failover command interface information
State	Show failover internal state information
Statistics	Show failover command interface statistics information

Some of the more frequently used commands are detailed below:

show failover	This command serves as a starting point for troubleshooting and provides a detailed summary of all aspects of the failover pair. These include whether failover is enabled, the current unit's configured role (primary or secondary), the failover interface and its status, polling timer values, software versions of both units, timestamp of last failover event, active and standby status of both units, how long the currently active unit has been active, and all monitored interfaces and their status and statistics related to stateful failover.

An example of the command output is shown below:

```
SECDCFRW1# show failover
Failover On
```

```
Failover unit Secondary
Failover LAN Interface: FAILOVER GigabitEthernet0/5 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 216 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.2(3)4, Mate 9.2(3)4
Last Failover at: 17:51:39 CST Feb 24 2016
        This host: Secondary - Active
                Active time: 1629887 (sec)
                slot 0: ASA5525 hw/sw rev (1.0/9.2(3)4) status (Up Sys)
                  Interface management (10.27.1.8): Normal (Monitored)
                  Interface SCADA-A (192.168.120.1): Normal (Monitored)
                  Interface L3VPN-SCADA-A (192.168.122.253): Normal (Monitored)
                  Interface L3VPN-SCADA-B (192.168.123.253): Normal (Monitored)
                  Interface CDC_DSS (192.168.125.1): Normal (Monitored)
        Other host: Primary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5525 hw/sw rev (1.0/9.2(3)4) status (Up Sys)
                  Interface management (10.27.1.9): Normal (Monitored)
                  Interface SCADA-A (192.168.120.2): Normal (Monitored)
                  Interface L3VPN-SCADA-A (192.168.122.254): Normal (Monitored)
                  Interface L3VPN-SCADA-B (192.168.123.254): Normal (Monitored)
                  Interface CDC_DSS (192.168.125.2): Normal (Monitored)

Stateful Failover Logical Update Statistics
        Link : FAILOVER GigabitEthernet0/5 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         5665710    0          217298     0
        sys cmd         217298     0          217298     0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1489073    0          0          0
        UDP conn        1376485    0          0          0
        ARP tbl         2496807    0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        VPN IKEv1 SA    0          0          0          0
        VPN IKEv1 P2    0          0          0          0
        VPN IKEv2 SA    0          0          0          0
        VPN IKEv2 P2    0          0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
        SIP Session     0          0          0          0
        Route Session   86046      0          0          0
        Router ID       0          0          0          0
        User-Identity   1          0          0          0
        CTS SGTNAME     0          0          0          0
        CTS PAC         0          0          0          0
        TrustSec-SXP    0          0          0          0
        IPv6 Route      0          0          0          0
        STS Table       0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       13      217298
        Xmit Q:         0       30      6533086
SECDCFRW1#
```

show failover history	This command provides a timestamped history for the current unit of all state changes since coming online. If a unit is in an unexpected or failed state, this command can indicate what happened just before the unit arrived at this state. An example of the command output for a normally functioning active unit is shown below.

```
SECDCFRW1# show failover history
==========================================================================
From State                To State                  Reason
==========================================================================
18:37:06 UTC Jan 11 2016
Not Detected              Negotiation               No Error

18:37:09 UTC Jan 11 2016
Negotiation               Just Active               No Active unit found

18:37:09 UTC Jan 11 2016
Just Active               Active Drain              No Active unit found

18:37:09 UTC Jan 11 2016
Active Drain              Active Applying Config    No Active unit found

18:37:09 UTC Jan 11 2016
Active Applying Config    Active Config Applied     No Active unit found

18:37:09 UTC Jan 11 2016
Active Config Applied     Active                    No Active unit found

==========================================================================
```

show failover state	This command provides the status of both members of the failover pair: whether configured as primary or secondary, and whether in active or standby mode. It also indicates the reason for the most recent failure event of either unit and the timestamp of that event. An example of the command output for a normally functioning failover pair is shown below.

```
SECDCFRW1# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  None

====Configuration State===
Sync Done
====Communication State===
Mac set
```

Remote Access Verification

This section describes remote access verification through Cisco Clientless SSL VPN and Cisco AnyConnect.

Cisco Clientless SSL VPN

This section describes remote access verification for a third party or remote worker user through Clientless SSL VPN.

Once the user uses VPN to access the corporate network (using AnyConnect or other flavor), the user makes use of the web browser to try to log in to the DSS zone. The user is then challenged with a certificate, which is authenticated before providing access to the servers in the DSS zone (Figure A-4 and Figure A-5). Access control policy in the firewall allows the third party user to have access to SCADA application servers in the DSS zone.

Figure A-4 SSL VPN Authentication

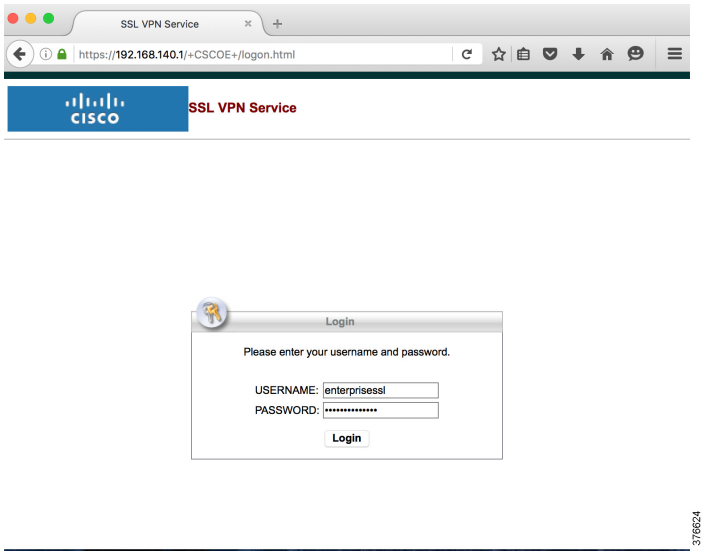
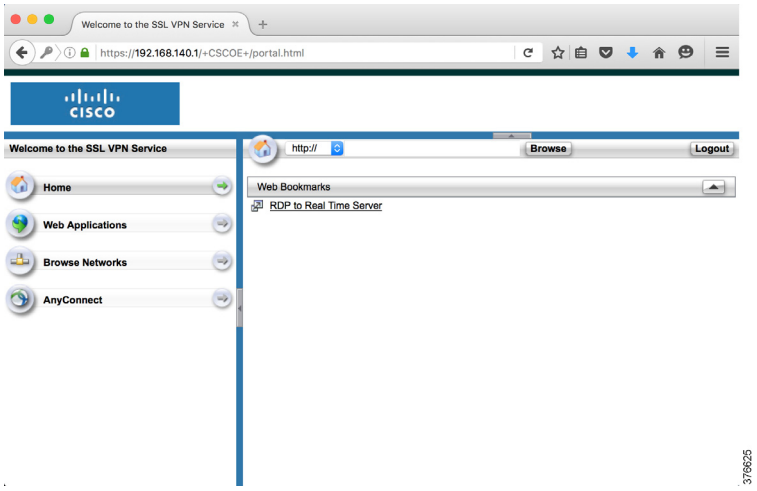


Figure A-5 Verification: SSL VPN Portal



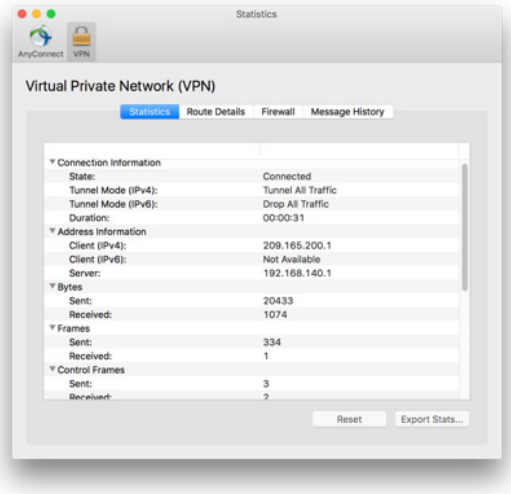
Cisco AnyConnect

This section describes remote access verification for an enterprise user through AnyConnect.

An Enterprise user uses the AnyConnect client to log into the DSS zone. The user is challenged with a certificate, which is authenticated, before being assigned an IP address from a pre-determined address pool (Figure A-6 and Figure A-7). Access control policies in the firewall allow the enterprise user to have access to SCADA application servers in DSS zone.

Figure A-6 Verification: Cisco AnyConnect Authentication

Figure A-7 Verification: Cisco AnyConnect VPN Statistics



Related Documentation

This Appendix includes the following major topics:

Unified Computing

Cisco UCS Manager GUI Configuration Guide, Release 2.2:

- http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/2-2/b_UCSM_GUI_Configuration_Guide_2_2.pdf
- http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/2-2/b_UCSM_GUI_Configuration_Guide_2_2.html

Cisco UCS Manager CLI Configuration Guide, Release 2.2:

- http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/cli/config/guide/2-2/b_UCSM_CLI_Configuration_Guide_2_2.pdf
- http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/cli/config/guide/2-2/b_UCSM_CLI_Configuration_Guide_2_2.html

Cisco UCS 6300 Series Fabric Interconnect Hardware Installation Guide:

- http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/6300-install-guide/6300_Series_HIG.pdf

Cisco UCS 5100 Series Blade Server Chassis Data Sheet

- http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-5100-series-blade-server-chassis/data_sheet_c78-526830.html

Cisco UCS 2304 Fabric Extender Data Sheet:

- http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-6300-series-fabric-interconnects/data_sheet_c78-675243.html

Cisco UCS B200 M4 Blade Server Data Sheet:

- http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b200-m4-blade-server/datasheet-c78-732434.html

Cisco UCS C220 M4 Rack Server Data Sheet:

- http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c220-m4-rack-server/datasheet-c78-732386.html

Network Infrastructure

Cisco ASR 900 Router Series Configuration Guide:

- http://www.cisco.com/c/en/us/td/docs/routers/asr903/software/guide/chassis/xe-3s/asr900-router-cfg-book.html

Cisco ASR 903 Router Chassis Software Configuration Guide:

- http://www.cisco.com/c/en/us/td/docs/wireless/asr_900/software/guide/chassis/ASR903-Chassis-SW.pdf

IP Routing: BGP Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series):

- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/asr903/irg-xe-3s-asr903-book.pdf

MPLS Basic Configuration Guide, Cisco IOS XE Release 3S (ASR 900):

- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_basic/configuration/xe-3s/asr903/mp-basic-xe-3s-asr903-book.pdf

Cisco Nexus 3548x and 3524x Switches Data Sheet:

- http://www.cisco.com/c/en/us/products/collateral/switches/nexus-3548-switch/data_sheet_c78-707001.html

Cisco Nexus 3548 Switch NX-OS Interfaces Configuration Guide, Release 6.x:

- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/interfaces/602_a1_1/b_N3548_Interfaces_Config_602_A1_1.pdf

Cisco Nexus 3548 Switch NX-OS Layer 2 Switching Configuration Guide, Release 6.x:

- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/layer_2_switching/60x/b_Cisco_N3548_Layer_2_Switching_Config_602_A1_1.pdf

Cisco Nexus 3548 Switch NX-OS System Management Configuration Guide, Release 6.x:

- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/system_mgmt/602/b_N3548_System_Management_Config_602A11.pdf

Security

Cisco ASA 5505 Adaptive Security Appliance and ASA 5500-X Series Next-Generation Firewalls Data Sheet:

- http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-701253.html

Cisco ASA Series General Operations CLI Configuration Guide, 9.2:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli.pdf

Cisco ASA Series General Operations ASDM Configuration Guide, 7.3:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/asdm73/general/asa-general-asdm.pdf

Cisco ASA Series Firewall ASDM Configuration Guide, 7.3:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/asdm73/firewall/asa-firewall-asdm.pdf

Cisco ASA Series VPN ASDM Configuration Guide, 7.3:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/asdm73/vpn/asa-vpn-asdm.pdf

Configuring AnyConnect VPN Client Connections:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/vpn_anyconnect.html

Configuring Simple Network Management Protocol (SNMP):

- http://www.cisco.com/c/en/us/td/docs/app_ntwk_services/data_center_app_services/css11500series/v8-20/configuration/administration/guide/admgd/SNMP.html

Configuring Secure Shell on Routers and Switches Running Cisco IOS:

- http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html#sshvvs

Network Time Protocol

Windows Time Service Technical Reference:

- https://technet.microsoft.com/en-us/library/cc773061%28v=ws.10%29.aspx

Network Time Protocol: Best Practices White Paper:

- http://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html

Windows Time Service Technical Reference:

- https://technet.microsoft.com/en-us/library/cc773061.aspx

Acronyms and Initialisms

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

Table C-1 Acronyms and Initialisms

Term	Definition
ASA	Adaptive Security Appliances
ASDM	Adaptive Security Device Manager
ASR	Cisco Aggregation Services Router
BGP	Border Gateway Protocol
BLISS	Base Line Integrated SCADA System
CIMC	Cisco Integrated Management Controller
CSV	Cluster Shared Volume
CVD	Cisco Validated Design
DSS	Decision Support System
DTP	Dynamic Trunk Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ePLM	Enterprise Pipeline Management
HBA	Host Bus Adapter
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zone
KVM	Kernel-based Virtual Machine
L3VPN	Layer 3 Virtual Private Network
LACP	Layer Aggregation Control Protocol
LLD	Low Level Design
LUN	Logical Unit Numbering
MPLS	Multiprotocol Label Switching
OOB	out-of-band
OSPF	Open Shortest Path First
P2P	peer-to-peer
PLC	Programmable Logic Controller

Table C-1 Acronyms and Initialisms (continued)

Term	Definition
PMS	Pipeline Management System
RCS	Remote Client Server
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SSH	Secure shell
SSL	Secure Sockets Layer
UCS	Cisco Unified Computing System
UCSM	Unified Computing System Manager
UDLD	Unidirectional Link Detection
VHD	Virtual Hard Disk
vNIC	virtual Network Interface Card
vPC	Virtual Port Channel
VRF	Virtual Routing and Forwarding
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network