RCMP ROYAL CANADIAN MOUNTED POLICE

Systems Delivery and Project Portfolio Management (SDPPM)

AFIS RENEWAL

Annex A to Appendix A: Current Architecture

Last Updated Date:	2016-06-08
Status:	Final
Version:	2
RDIMS Document No.:	42072v8b

TABLE OF CONTENTS

FIGURES

1. INTRODUCTION

1.1 Purpose

1. The purpose of document is to describe the current RCMP/SSC architecture within which RTID operates. The AFIS renewal and all its subsystems must operate effectively within this RCMP/SSC architecture and satisfy all the requirements stated in this SOW.
2. This document provides a brief high-level description of the RCMP/SSC architecture and a more focused description of the RCMP/SSC architecture related to the AFIS components.

1.2 General

1. The RCMP performs a crucial role in the collection, storage and management of police related information. The National Police Services Network (NPSNet) provides the means by which the Canadian law enforcement organizations may electronically access this centrally located information. NPSNet also supports internal RCMP applications. NPSNet provides national network support to the RCMP and its business affinity partners over a private dedicated network. NPSNet provides network services for the transport of electronic information in support of the operational and administrative services used by the client organizations. It serves approximately 60,000 users in approximately 1200 locations across Canada and the high Arctic.
2. NPSNet also provides connectivity to national police agencies, international police forces, Canadian federal, provincial and municipal organizations as well as private agencies requiring RTID capabilities. These connections are provided through a secure private VPN controlled and managed by Shared Services Canada (SSC) called the National Security Posture (NSP) and through establishing VPNs through the GC Secure Channel Network (SCNet) or through secure VPNs through the Internet. All RTID agency connectivity is through one of these methods, which will be described throughout this document.

1.3 Document Organization

1. This document provides a brief high-level description of the RCMP architecture. Following this high-level architecture, a description of the current AFIS and VSS architecture is presented.
2. The AFIS and VSS architecture are described at a high-level followed by detailed diagrams and descriptions of the connectivity between various AFIS and VSS components including the interfaces with RTID and RCMP/SSC components.

2. RCMP/SSC HIGH-LEVEL ARCHITECTURE

2.1 RCMP/SSC Conceptual Security Architecture

1. Figure 2-1 depicts a conceptual view of the RCMP/SSC security architecture within which RTID operates. Any details concerning the security architecture that are applicable to RTID were discussed at the industry day associated with this AFIS Renewal SOW.

2. This diagram depicts the private dedicated RCMP network NPSNet as well as the NSP and SCNet / Internet VPN connectivity for external agencies.

3. Note: Some sites are being migrated from a VPN connection to secure Multi-Protocol Label Switching (MPLS); however, there is no impact on RTID or AFIS. This is just an alternate method to establish a secure encrypted connection.

4. The diagram depicts the RTID devices that are used through the different types of connectivity.

5. Additionally, the diagram depicts a conceptual view of where NNS and the AFIS components are located within the RCMP/SSC architecture.

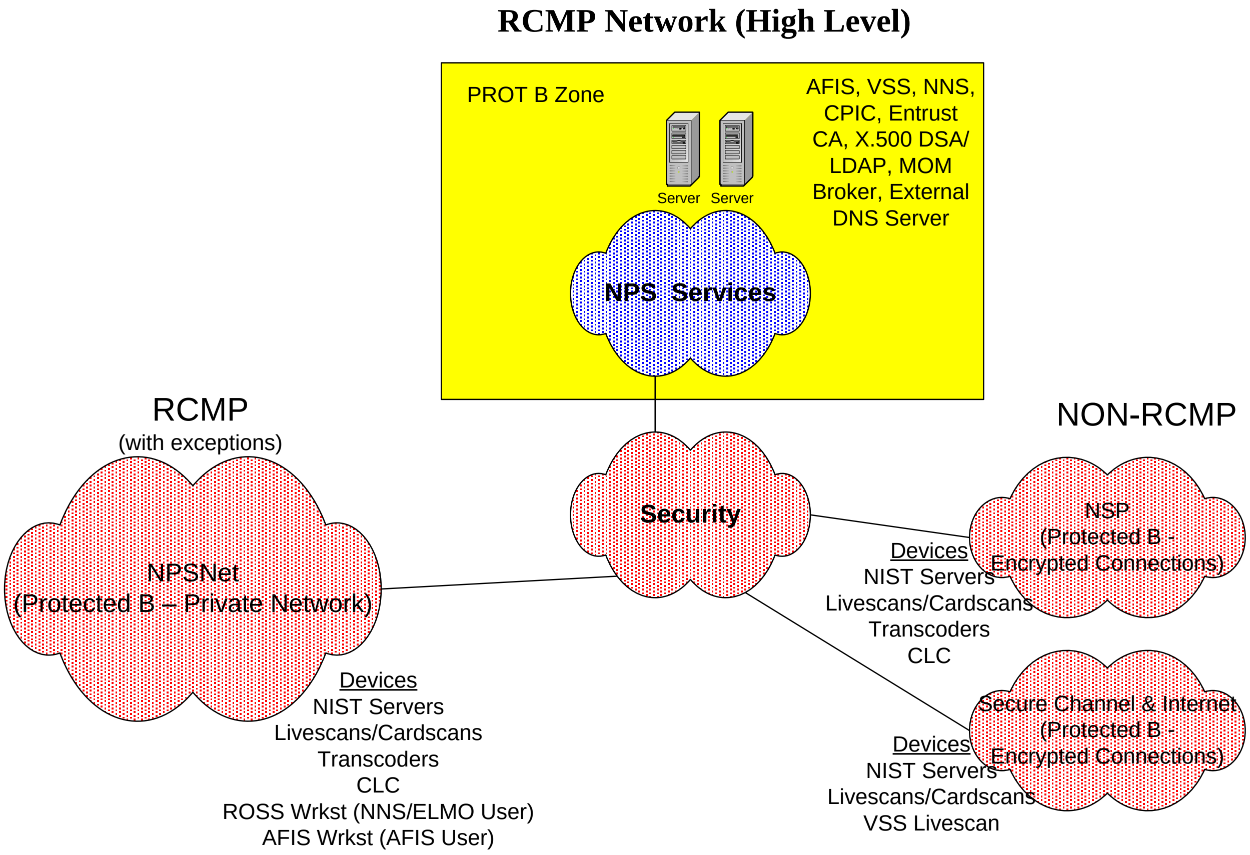
RCMP Network (High Level)
PROT B Zone
Server
Server
AFIS, VSS, NNS, CPIC, Entrust CA, X.500 DSA/ LDAP, MOM Broker, External DNS Server
NPS Services
RCMP
(with exceptions)
NON-RCMP
Security
NPSNet
(Protected B – Private Network)
NSP
(Protected B - Encrypted Connections)
Devices
NIST Servers
Livescans/Cardscans
Transcoders
CLC
Devices
NIST Servers
Livescans/Cardscans
Transcoders
CLC
ROSS Wrkst (NNS/ELMO User)
AFIS Wrkst (AFIS User)
Secure Channel & Internet
(Protected B - Encrypted Connections)
Devices
NIST Servers
Livescans/Cardscans
VSS Livescan

Figure 2-1: RTID Conceptual Architecture

2.2 RTID Security Within the RCMP Architecture

2.2.1 ENCRYPTION

1. All RTID data transmitted outside the Protected B security zone must be encrypted to/from the contributing agency or to/from the RTID NNS users.
2. NPSNet is a secure MPLS private network for RCMP/SSC use.
3. NSP is an extension of the RCMP/SSC network, typically referred to as a managed LAN. RCMP/SSC controlled and managed VPNs at each site allow capabilities including RTID to be extended to non-RCMP sites with secure communications.
4. SCNet is a GC-controlled and managed secure communication network using VPNs. RCMP/SSC enables connectivity with other government departments that require access to RTID.
5. Additionally, permanent and temporary VPNs can be established through an Internet connection for private agencies submitting to RTID.

2.2.2 IDENTIFICATION AND AUTHENTICATION

1. Direct RTID user access requires two-factor authentication. Either a certificate (token or smart card) and password; or a biometric and password is required for authenticating users that access RTID.
2. AFIS user workstations are within an isolated Protected B zone; therefore, there are no encryption requirements for the communication between the AFIS workstations and the AFIS/VSS servers. AFIS users are authenticated with two-factor authentication using a biometric and password. Only RCMP users within the AFIS/VSS VLAN have access to AFIS.
3. Individuals on NSP, SCNet or the Internet can establish a temporary VPN using a token or smart card as two-factor authentication to be able to send RTID submissions and receive RTID responses through an SMTP/POP interface. Transcoder users use permanent encrypted VPNs and establish a session using a biometric and password, as two-factor authentication, to be able to send RTID submissions and receive RTID responses through an SMTP interface. These users can only send and receive email with RTID through a secure VPN. They do not have any RTID/NNS/AFIS user capabilities.

2.3 RTID Load Balancing and Network Address Translation

1. For security, performance, scalability and load balancing reasons, the RCMP has implemented OSI layers 4–7 content switching with load balancing and Network Address Translation (NAT) support through network devices configured with LB/SSL modules. This load balancing enables application and/or service requests to be directed to a virtual server and then distributed to multiple servers managed by the load balancing. NAT allows the IP addresses of the real servers to be concealed and transparent to the requester. NAT translates the IP address used in the request to the IP addresses of the real servers. This combination of services allows requests to be

sent to a Virtual IP address (VIP) to conceal the real IP address and greatly improve performance by creating a scalable environment. This capability is also used to direct requests, based on content to the appropriate server. Additionally this network-level load balancing inherently provides intra-site and inter-site fail-over at the network level. Additionally, the AFIS/VSS servers send responses to a VIP. These are critical requirements that must be supported by the Contractor's AFIS renewal solution proposed to satisfy the requirements in this SOW.

2.4 Current High-Level RTID Architecture

1. Figure 2-2: Current RTID High-Level Architecture, depicts the RTID components. It is presented herein to show the relationship between the RCMP/SSC conceptual security architecture, the RTID components and the architecture diagrams for the AFIS components that follow in the next section.
2. A brief description of each component was provided in the Appendix A SOW for this AFIS Renewal.

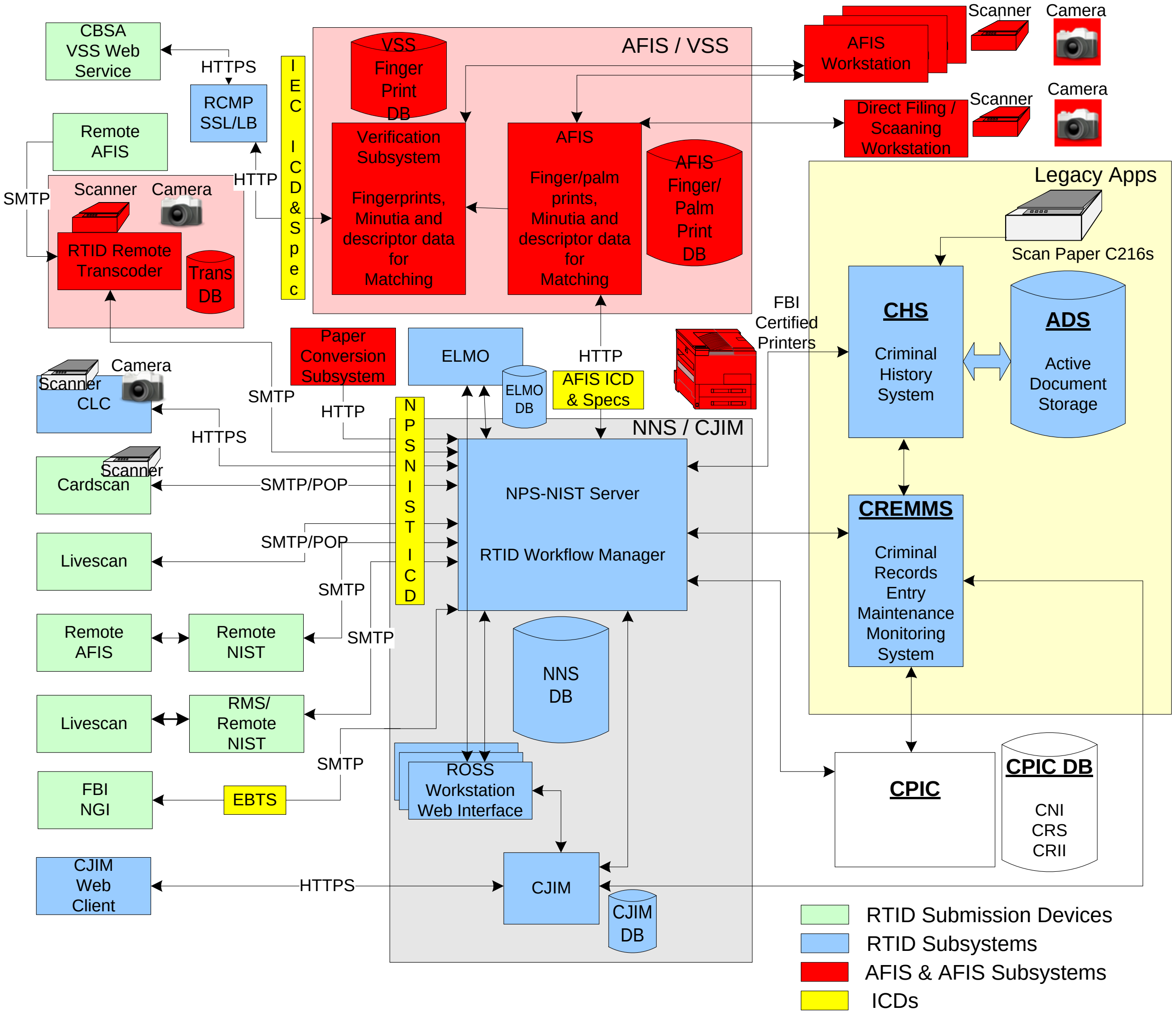

Figure 2-2: Current RTID High-Level Architecture

3. AFIS AND VSS ARCHITECTURE

3.1 AFIS and VSS Immigration Conceptual Architecture

1. The following diagram depicts the conceptual architecture for AFIS and VSS. This diagram specifically depicts IRCC (previously CIC) and CBSA as the contributors of fingerprints that are enrolled. This is the common RTID SMTP interface used by most contributors. IRCC submit ninety-nine percent (99%) of the Immigration (formerly TRB) enrolments, with CBSA sending Refugee submissions that are processed internally within RTID/AFIS like IMM enrolments.

2. IRCC capture fingerprints for individuals seeking entry to Canada. IRCC submit Immigration (IMM) NIST packets with the individuals fingerprints and a unique identification number. These fingerprints are enrolled in AFIS and a copy of the fingerprints is sent to VSS. When the individual arrives at a Port Of Entry (POE), CBSA captures the individual's fingerprints with their unique identification number and transmits the Verification (VER) NIST packet to VSS for comparison against the fingerprints previously captured by IRCC.

3. Any purges (Immigration Purge – IMP) submitted by IRCC will also purge the fingerprints from VSS.

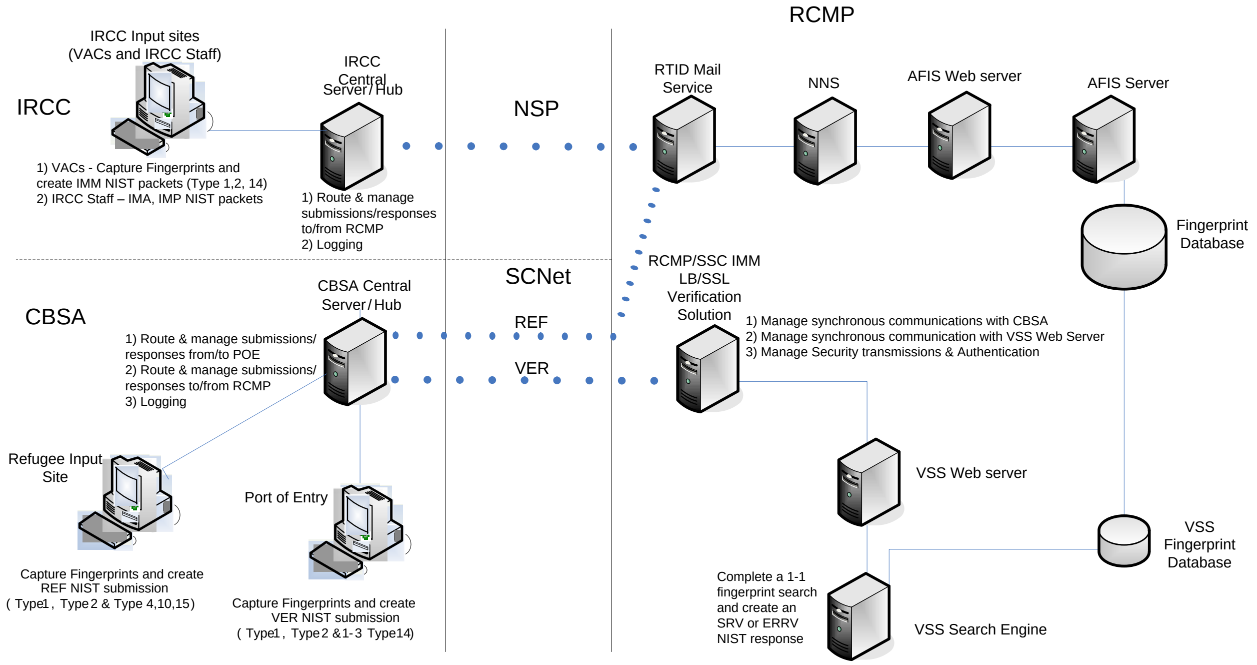
RCMP
IRCC Input sites
(VACs and IRCC Staff)
IRCC
IRCC Central Server/Hub
NSP
RTID Mail Service
NNS
AFIS Web server
AFIS Server
1) VACs - Capture Fingerprints and create IMM NIST packets (Type 1,2, 14)
2) IRCC Staff – IMA, IMP NIST packets
1) Route & manage submissions/responses to/from RCMP
2) Logging
Fingerprint Database
SCNet
RCMP/SSC IMM LB/SSL Verification Solution
CBSA
CBSA Central Server/Hub
REF
VER
1) Route & manage submissions/ responses from/to POE
2) Route & manage submissions/ responses to/from RCMP
3) Logging
1) Manage synchronous communications with CBSA
2) Manage synchronous communication with VSS Web Server
3) Manage Security transmissions & Authentication
Refugee Input Site
Port of Entry
VSS Web server
VSS Fingerprint Database
Capture Fingerprints and create REF NIST submission (Type1 , Type2 & Type 4,10,15)
Capture Fingerprints and create VER NIST submission (Type1 , Type2 &1-3 Type14)
Complete a 1-1 fingerprint search and create an SRV or ERRV NIST response
VSS Search Engine

Figure 3-1: RTID / AFIS / VSS IRCC / CBSA Conceptual Architecture

3.2 AFIS and VSS High-Level Architecture

1. Figure 3-2 depicts the high-level architecture of AFIS and VSS as well as the RTID components with which they interface. The RTID solution is designed based on ICDs and the ability to add or replace components based on adherence to the ICD.

2. AFIS and VSS can operate independently with the exception that fingerprint enrolments, purges or other updates are only through the AFIS; and AFIS communicates the Immigration related fingerprints, purges and updates to VSS. That is, AFIS can operate without VSS; however, AFIS updates to VSS will be queued until VSS is online. As well, VSS can operate without AFIS; however, no enrollments, purges or updates will be received without AFIS.

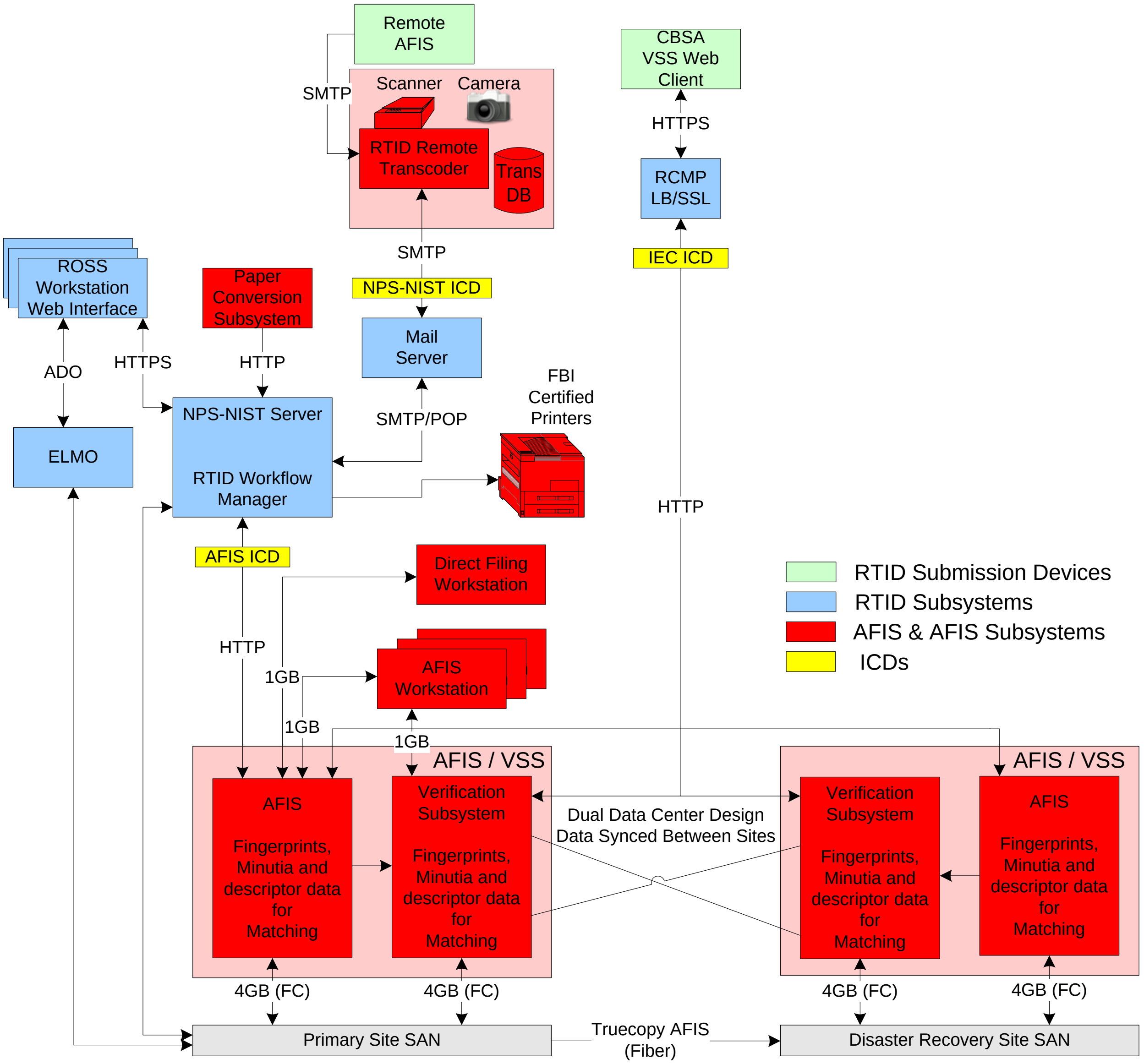

Figure 3-2: AFIS and VSS High-Level Architecture

3. AFIS is designed as a semi-automatic fail-over Disaster Recovery (DR) site solution. Production AFIS components are operating at both the Primary (PR) site and the DR site. All required AFIS DB and file system files are mirrored to the DR site. In case of a disaster, AFIS will be restarted using the AFIS components at the DR site. The entire RCMP/SSC security/network infrastructure automatically fails over to the DR site therefore allowing the AFIS components to interface with any available RTID components. The AFIS DR components are in the same security zone as the PR components; therefore, the security architecture is maintained across both sites.

4. VSS is designed as a dual data center model with an automatic fail-over DR site solution. VSS components at both the PR and DR sites are fully utilized to maximize the capabilities of all components to satisfy the performance requirements. As depicted in the above high-level architecture, the RCMP/SSC LB/SSL load balances evenly to both the PR and DR sites. In case of a disaster, VSS will simply operate with the VSS nodes at the DR site. The entire RCMP/SSC security/network infrastructure automatically fails over to the DR site; therefore, Production CBSA VSS contributors would not know that the PR site was inoperable. Regardless of whether it is the PR or DR site that is out of service for a period of time, both sites will resynchronize with each other automatically, to ensure that both sites have the same data. This resynchronization occurs as soon as the service is restored and typically completed within five-ten (5–10) minutes. As a dual data center model VSS components fully operate within the same security zone as AFIS.

5. All AFIS workstations have one (1) GB connections.

6. AFIS and VSS servers have four (4) GB connection to the SAN.

7. There is fiber optic cabling between the PR and DR site.

3.3 AFIS and VSS Test Environments

3.3.1 GENERAL

1. RTID Test environments include AFIS, VSS, NNS and all other components required to test any RTID changes destined for the Production environment.

2. There are three (3) AFIS test environments, DEVTEST, Quality Control Section (QCS) and MAINT. Each AFIS test environment can support multiple RTID NNS environments.

3. The AFIS DEVTEST and MAINT environments support multiple NNS environments. This special configuration is available in all test environments; however, typically it is only used in the AFIS DEVTEST and MAINT environments.

4. The AFIS DEVTEST environment supports multiple NNS Integration environments, multiple NNS SYSTEST environments, multiple NNS performance environments and multiple individual developer environments. The special configuration enables the DEVTEST AFIS to interface with individual developer environments or to an NNS environment. This is a critical capability that allows developers to interface with the AFIS DEVTEST environment to satisfy their specific test/development requirements; and to complete development and release testing of the AFIS changes together with the NNS portion of RTID.

5. The RTID SYSTEST1 environment is used to test any RTID changes destined for the Production environment through the normal release process. SYSTEST1 is the primary test environment for all RTID components. Once successfully tested in the SYSTEST1 environment, changes will be tested in the RTID QCS environment.

6. The AFIS QCS environment supports one (1) RTID NNS QCS environment. The AFIS QCS environment is configured with every possible AFIS components operating in the Production environment. The AFIS components in QCS allow for every possible Production issue to be tested. That is, at least one (1) AFIS component exists in the QCS environment for every unique type of components in the Production environment to ensure every possible Production issue can be verified and the correction tested effectively.

7. The AFIS MAINT environment primarily supports an NNS Maintenance and NNS Certification environment; however, it is capable of supporting additional environments.

8. The AFIS MAINT environment primarily supports an NNS Maintenance and NNS Certification environment; however, it is capable of supporting additional environments. The Certification environment is used to certify vendor and contributor systems against the NPS-NIST ICD and the ICD for IEC. Consequently, the NNS Certification environment has the same version of NNS software as Production. The NNS Certification environment is updated two (2) weeks after an NNS Production release. The NNS Maintenance environment has the same version of NNS software as Production until one (1) week prior to an NNS production release.

9. For AFIS and VSS releases, the AFIS MAINT environment is used to install, configure and implement new AFIS and VSS releases and changes prior to implementation in the AFIS DEVTEST environment. This ensures AFIS and VSS changes are initially tested against stable NNS software. Two (2) weeks after successful deployment to Production any AFIS changes required during the release testing process are deployed in the AFIS MAINT environment.

10. Each AFIS environment is configured with the quantity of workstations and Transcoders necessary to effectively test any changes. The following diagrams depict the number of workstations/Transcoders in each environment.

3.3.2 AFIS AND VSS DEVTEST

1. Figure 3-3 depicts the AFIS DEVTEST environment architecture.

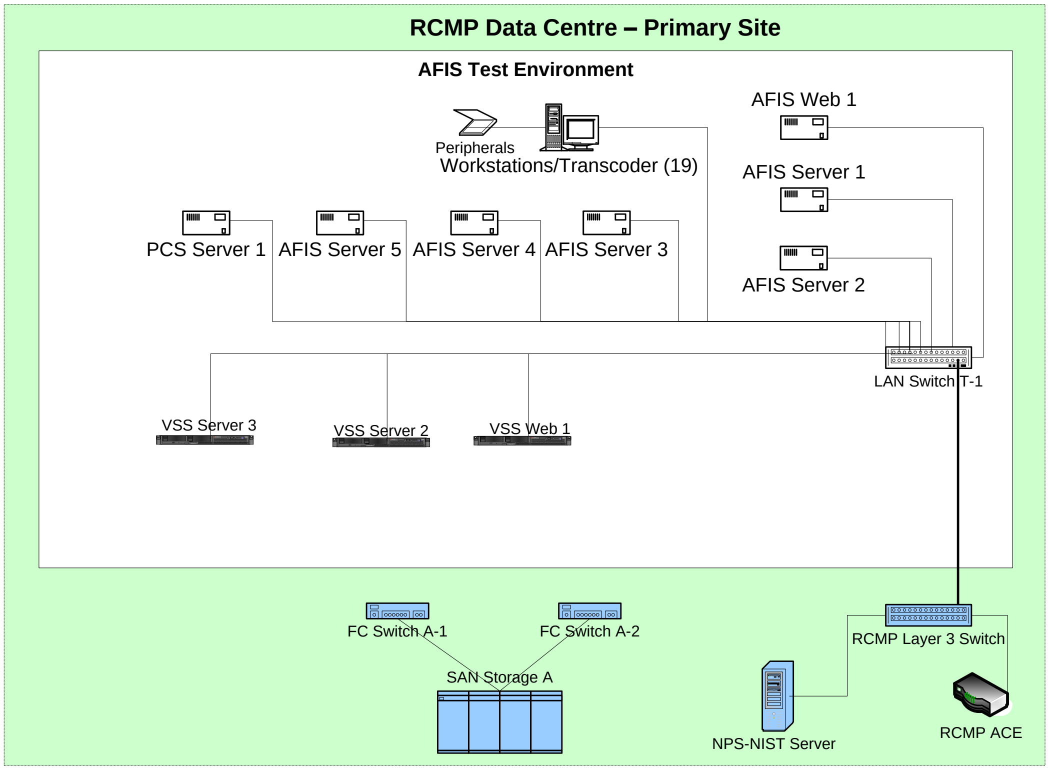

Figure 3-3: Development and Test Environment

2. The interface between the NNS and AFIS system is through the NNS Web server capability and the AFIS Web servers.

3. The RCMP/SSC's LB/SSL provides a secure connection between CBSA and RCMP for the VSS. The LB/SSL is also used to interface with the VSS Web server and together with the VSS Web server maintain a synchronous connection that provides results from the VSS Web server to CBSA. IRCC and CBSA perform ongoing testing in the RTID test environments. They require the interface to test any changes to their systems or changes to RTID that potentially affect them. As well, other agencies occasionally test in the RTID test environments. All external agency access to the test environments is also through one of the secure connections previously identified. These external agency test connections are configured as Production controlled interfaces even though they access test systems.

4. Refer to the TRB Verification Interface Specifications (RDIMS #38553) for details concerning the interface between CBSA, the LB/SSL and the Contractor's VSS Web servers.

5. Note: For proprietary reasons only generic names for the servers are used in the diagrams.

3.3.3 AFIS AND VSS QUALITY CONTROL SECTION (QCS)

1. The QCS environment is used for QCS testing to confirm the operational readiness and stability of any changes prior to implementation in the Production Environment. Successful testing in this environment is required before implementation of the change/release in the Production environment. This QCS environment is the only test environment with High Availability (HA) configurations that allow failover/redundancy capabilities to be tested.

2. Figure 3-4 depicts the QCS architecture.

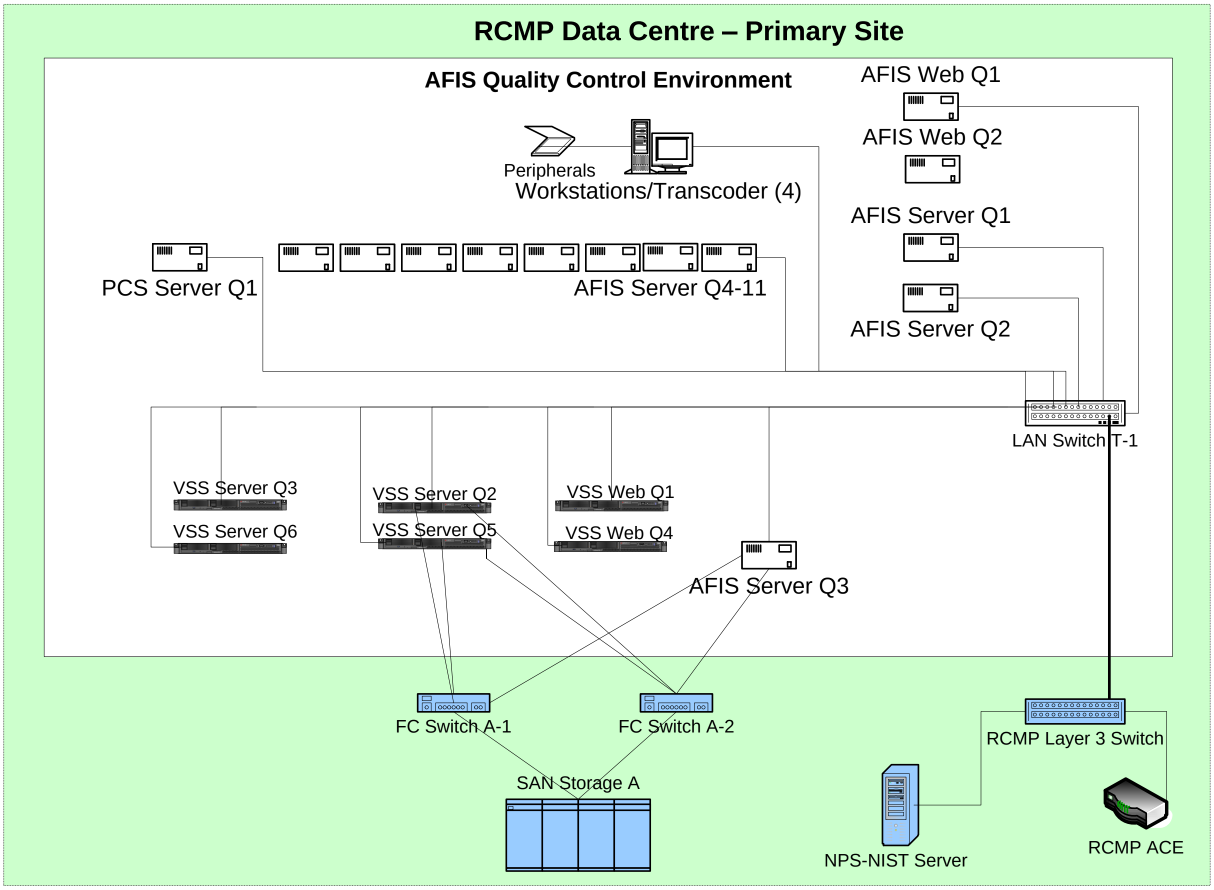

Figure 3-4: Quality Control Environment

3. The interface between the NNS and AFIS system is through the AFIS Web server.

4. The two (2) AFIS Web servers in this QCS environment allow automated HA testing to be performed that allows services to fail-over between Web servers.

5. There are three (3) sets (two (2) of each type) of latent fingerprint matching components that allow various HA scenarios to be tested for latent processing.

6. The VSS servers are configured as two (2) nodes (with four (4) nodes configured in production), allowing multiple node HA testing to be performed to allow the production solution to be effectively tested in the QCS environment.

7. The QCS VSS connection is normally tested with an internal client that simulates the CBSA connection. RCMP/SSC's LB/SSL provides the secure connection between the internal client and VSS in the same manner as it does for the CBSA connection. The LB/SSL is also used to interface with the QCS VSS Web servers, load balance traffic between the two (2) VSS Web servers and maintain a synchronous connection that provides results from the VSS Web servers to the internal client.

8. The RCMP/SSC's LB/SSL is also used to provide load balanced communication from NNS to AFIS, from AFIS to NNS and between AFIS components to create a scalable HA configuration through the RCMP/SSC's network infrastructure.

9. There are a few scenarios for which HA testing cannot be performed in the QCS environment. These scenarios involve one (1) component that fully satisfies the requirements at a site or a proprietary mechanism to fully utilize the devices without requiring infrastructure load balancing or network level fail-over. For example Ten-Print (TP) fingerprint processing uses one (1) device to fully support the capacity requirements for RTID at a site; therefore, there is no infrastructure load balancing. There is also one (1) TP device at the DR site which is fully utilized through a proprietary mechanism. Since this fail-over is tested yearly and the TP HA test requires an RCMP/SSC infrastructure fail-over to effectively test, it is not tested in the QCS environment. Additionally, cluster fail-over testing of AFIS functional servers are only tested in Production. Since the DR AFIS functional servers are only used in case of a failure, these DR servers can be used to test any cluster related issues without affecting production operations.

10. Note: On a yearly basis RCMP/SSC performs a complete DR site fail-over test where the network and all applications are verified to operate at the DR site. This yearly test is used to test all AFIS and VSS fail-over to ensure all capabilities operate at the DR site. This allows AFIS and VSS HA capabilities that cannot be tested in the QCS environment to be tested with the RCMP/SSC network infrastructure fail-over and AFIS DR operation with the SAN mirrored database and file system data.

3.3.4 AFIS AND VSS MAINTENANCE

1. The NNS Maintenance and Certification environments have the latest Production release of NNS and all other non-AFIS components enabling AFIS changes to be verified against the current production release that matches the production environment. For AFIS and VSS releases, the AFIS Maintenance environment is used to install, configure and implement new AFIS and VSS releases and changes prior to implementation in the DEVTEST environment.

2. This AFIS Maintenance environment is used to verify the Contractor changes function as designed and ensure the Contractor components continue to interface correctly with the NNS. Successful testing in this environment is required before implementation of the release in the DEVTEST environment.

3. Figure 3-5 depicts the Maintenance architecture.

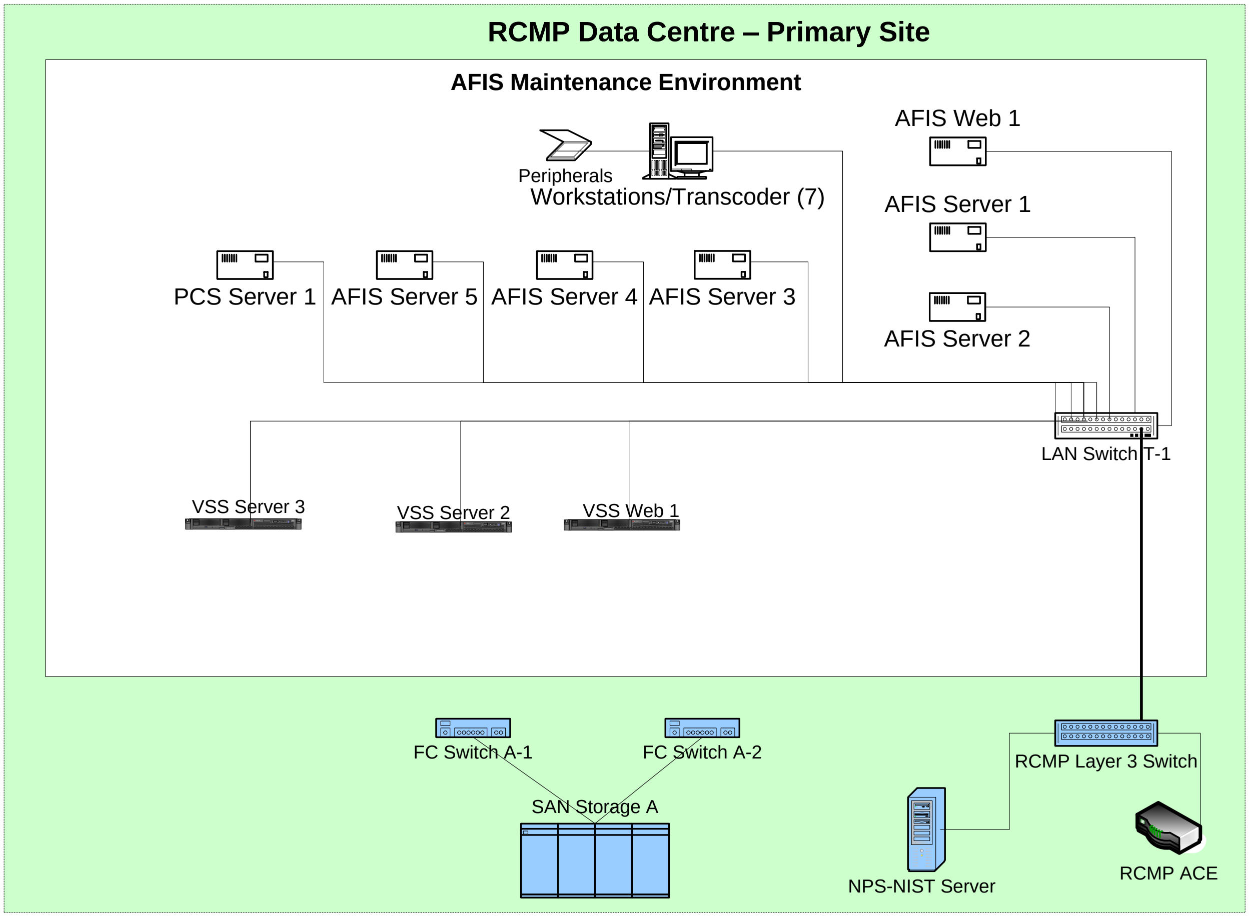

Figure 3-5: Maintenance Environment

4. The interface between the NNS and AFIS system is through the NNS Web server capability and the AFIS Web servers.

5. The RCMP/SSC's LB/SSL provides a secure connection between CBSA and RCMP for the VSS. The LB/SSL is also used to interface with the VSS Web server and maintain a synchronous connection that provides results from the VSS Web server to CBSA. On an exceptional basis, IRCC and CBSA will test in the Maintenance environment when the DEVTEST environment cannot be used to effectively support the conditions under which they need to test.

3.4 AFIS and VSS Production Environment

3.4.1 GENERAL

1. The AFIS and VSS production environment includes a Primary (PR) site and a Disaster Recovery (DR) site that supports all AFIS and VSS production capabilities. Figure 3-6 depicts the PR/DR architecture.

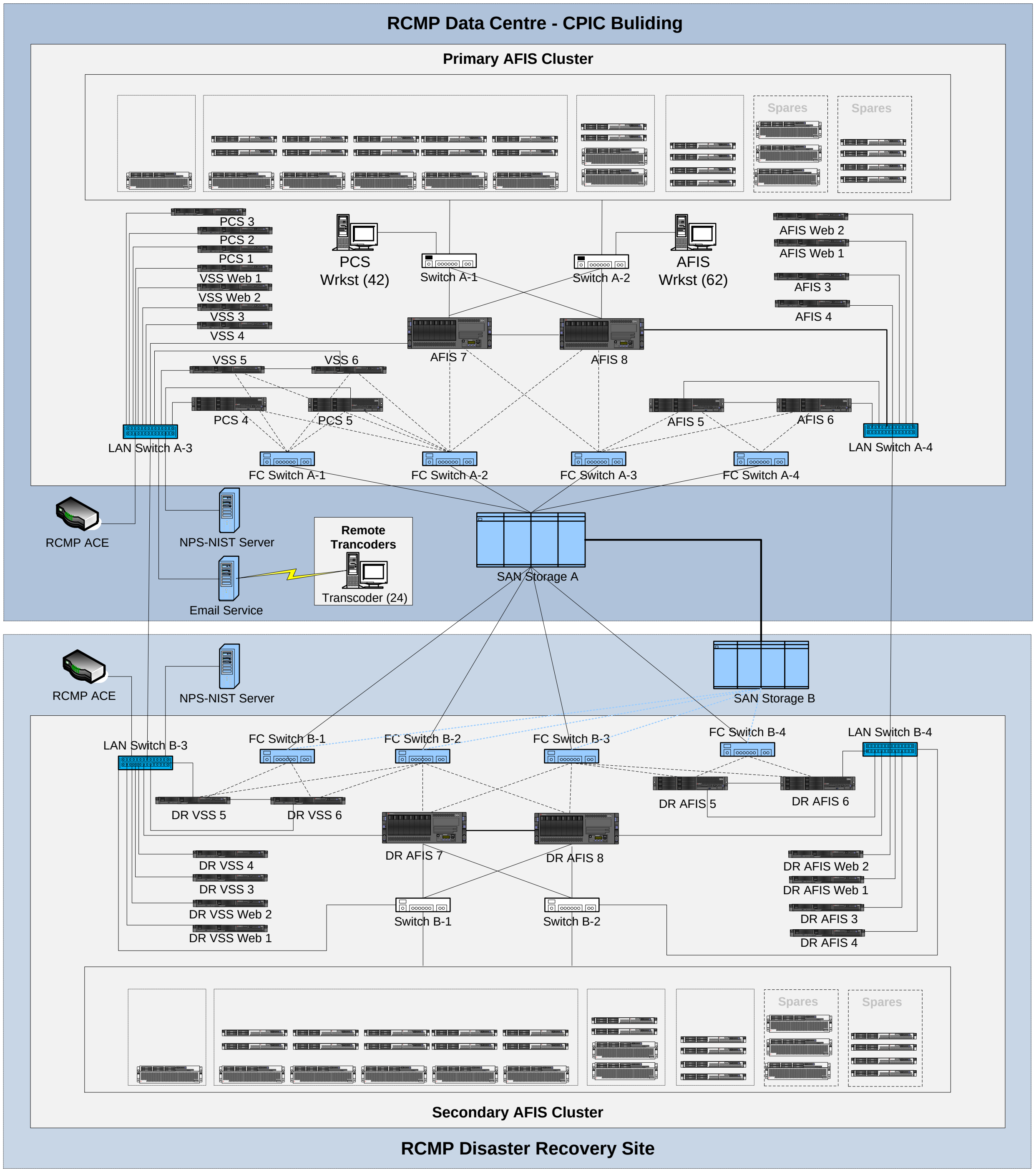

Figure 3-6: Production Architecture

2. All AFIS PR and DR matching components are fully utilized as part of normal operations. This creates a pseudo dual data center architecture where all matching components at both sites are utilized. The DR Web servers and the DR AFIS functional servers are only used if the PR site fails and operations have to be re-established at the DR site with the SAN mirrored data. In case of a PR site failure, the DR Web and DR AFIS functional servers would use the fingerprint matching components at DR only.

3. VSS is a fully automated dual data center architecture that utilizes all servers at PR and DR and does not require any manual intervention to recover from a site failure. The integrated database exists at both the PR and DR sites enabling each site to work together or independently in case of a failure. The sites automatically resynchronize the integrated database once both sites are operational.

4. The AFIS and VSS test and Production environments are integrated with RCMP/SSC maintenance and support capabilities. This integration is critical to the effective operation of AFIS and VSS within the RCMP/SSC infrastructure. The following subsections identify capabilities that the RCMP/SSC infrastructure supports for all AFIS and VSS test and Production environment components.

3.4.2 PRODUCTION PRIMARY (PR) SITE

1. The PR environment is used to support the production operational environment of AFIS and VSS. The PR/DR supports HA configurations that allow failover/redundancy capabilities within each site and between sites to ensure there is no single point of failure.

2. The interface between the NNS and AFIS is load balanced through the LB/SSL to the AFIS Web servers. The interface between the AFIS and NNS is load balanced through the LB/SSL to the NNS Web servers.

3. The two (2) AFIS Web servers at the PR site provide HA capability. As well, all other AFIS functional servers are configured as pairs to provide HA capabilities within each site.

4. The PR site AFIS functional servers utilize all matching components (excluding live spares) at both the PR and DR site providing HA capabilities.

5. The RCMP/SSC's LB/SSL provides a secure connection between CBSA and RCMP for the VSS. The LB/SSL is also used to load balance and interface with the PR and DR VSS Web servers; and maintain a synchronous connection that provides results from the VSS Web server to CBSA. This VSS architecture is an automated dual data center configuration providing HA capabilities within a site and between sites.

3.4.3 DISASTER RECOVERY (DR)

1. The DR is configured with all the same servers as PR except for the PCS. As well, there are no workstations or other peripherals at the DR site. Workstations and other peripherals can easily be installed and configured to support DR only operations.

3.4.4 BACKUP AND RESTORE

1. RCMP/SSC has comprehensive backup and restore capabilities that are used by the AFIS and VSS databases and file system data. These capabilities include Tivoli Storage Management (TSM) and SAN mirroring.

3.4.5 SNMP REPORTING

1. All AFIS and VSS servers support SNMP reporting capabilities. Production and QCS environment servers have enabled reporting to RCMP/SSC's Spectrum/eHealth system monitoring solution. Additionally, some DEVTEST and MAINT servers also have enable reporting to RCMP/SSC's Spectrum/eHealth to ensure test servers are monitored allowing uninterrupted DEVTEST and MAINT environment services.

2. This SNMP reporting includes automated system level monitoring capabilities at the hardware and software application level, capable of producing SNMP traps/alerts when software or hardware faults are detected. The minimum SNMP reporting includes memory utilization, CPU utilization, disk utilization, key process failures and hardware faults.

3.4.6 MCAFEE ANTI VIRUS (AV) SCANNING

1. All AFIS and VSS servers and workstations, in all environments, receive automatic AV updates from the RCMP/SSC McAfee AV scanning through participation in ePo (ePolicy Orchestrator), with rare exceptions where the updates are completed manually in a manner approved by the RCMP with a configuration management documented history of the updates. These rare exceptions are for specialized components where the AV updates are verified in the QCS environment prior to updating the Production environment.

3.4.7 OS AND SOFTWARE UPGRADES

1. All AFIS and VSS Windows servers and workstations/transcoders, in all environments, receive Windows OS updates in an automated manner from RCMP/SSC Windows Server Update Services (WSUS). Workstation WSUS updates are forced within a specific timeframe if the user does not allow the updates to be completed prior to the time limit. Servers automatically receive the updates and AFIS and VSS support staff complete the updates during off hours.

2. For all non-Windows servers, RCMP/SSC provides approved patches and upgrades for the OS common software which is used to update the AFIS and VSS non-Windows servers. The AFIS and VSS support staff complete the updates during off hours.

3.4.8 DESIGNATED SPECIAL PORTS

1. The AFIS and VSS servers are also configured to use designated ports for various types of connectivity based on RCMP/SSC policy.