Systems Delivery and Project Portfolio Management (SDPPM)

EFCD RFSO

ANNEX A TO APPENDIX A: CURRENT ARCHITECTURE

Last Updated Date:	2019-03-09
Status:	Final
Version:	1.0
RDIMS Document No.:	45383v2a

TABLE OF CONTENTS

FIGURES

1. INTRODUCTION

1.1 Purpose

1. The purpose of this document is to describe the current RCMP/GC/CPMG architecture within which the EFCD/SMTP-SPOI/ RMS/DMS devices operate. The EFCDs and SMTP-SPOI servers must operate effectively within this RCMP/GC/CPMG architecture and satisfy all the requirements stated in this SOW.

2. This document provides a brief high-level description of the RCMP/GC/CPMG architecture and a more focused description of the RCMP/GC/CPMG architecture related to the EFCD/SMTP-SPOI devices.

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. All RTID agency connectivity is through one of the following methods which will be described throughout this document:

   a. Secure private VPN controlled and managed by Shared Services Canada (SSC) called the National Security Posture (NSP);

   b. Secure VPN through the GC Secure Channel Network (SCNet);

   c. Secure VPN through GC Cloud; or

   d. Secure VPN through the Internet..

1.3 Document Organization

1. This document provides a brief high-level description of the RCMP/GC/CPMG architecture within which EFCDs and SMTP-SPOI servers must operate.

2. Following this high-level architecture, a description of the connectivity that the EFCDs and SMTP-SPOI servers must support.

2. RCMP/GC/CPMG HIGH-LEVEL ARCHITECTURE

2.1 RCMP/GC/CPMG Conceptual Security Architecture

1. Figure 2-1 depicts a conceptual view of the RCMP/SSC security architecture within which EFCD/SMTP-SPOI devices must operate.

2. Some GC/CPMG departments/agencies have private networks similar to RCMP's NPSNet and many GC/CPMG departments/agencies have access to SCNet/GC Cloud. EFCD/SMTP-SPOI devices must operate within these private RCMP/GC/CPMG networks and through SCNet/GC Cloud.

3. The EFCD/SMTP-SPOI devices must be able to support all the requirements throughout the SOR and its accompanying documents to communicate within these various private networks or through the Internet to NIST servers within a department/agency or to RTID.

4. The diagram depicts the private dedicated RCMP network NPSNet as well as the NSP and SCNet / GC Cloud / Internet VPN connectivity for external agencies.

5. 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 the EFCD/SMTP-SPOI devices. This is just an alternate method to establish a secure encrypted connection.

6. The diagram depicts the applicable EFCD/SMTP-SPOI devices that are used through the different types of connectivity.

7. Additionally, the diagram depicts a conceptual view of the RTID components located within the RCMP/SSC architecture.

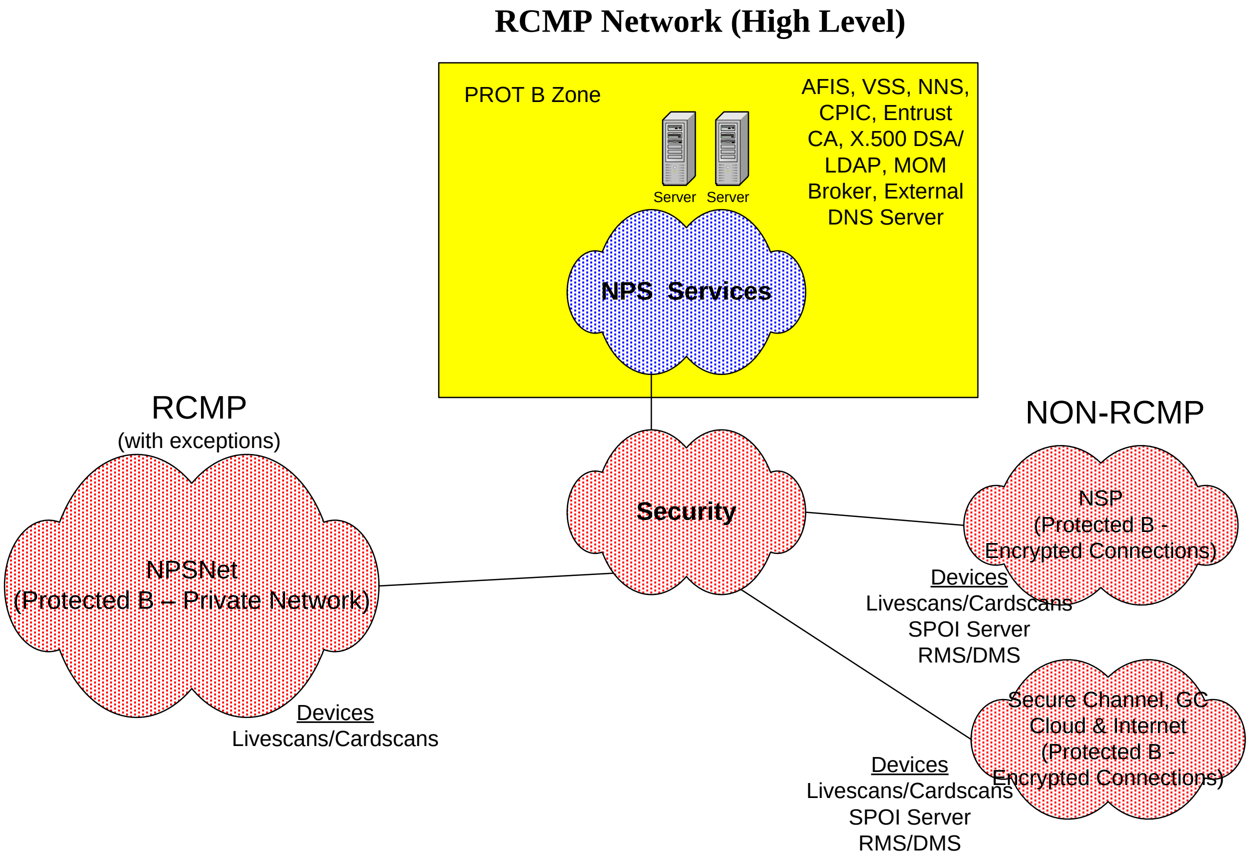
RCMP Network (High Level)
PROT B Zone
Server
Server
AFIS, VSS, NNS, CPIC, Entrust CA, X.500 DSA/ LDAP, MOM Broker, External DNS Server
NPS Services
RCMP
(with exceptions)
NPSNet
(Protected B – Private Network)
Devices
Livescans/Cardscans
Security
NON-RCMP
NSP
(Protected B - Encrypted Connections)
Devices
Livescans/Cardscans
SPOI Server
RMS/DMS
Secure Channel, GC Cloud & Internet
(Protected B - Encrypted Connections)
Devices
Livescans/Cardscans
SPOI Server
RMS/DMS

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 EFCD/SMTP-SPOI devices.
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/GC Cloud is a GC-controlled and managed secure communication network using VPNs. SCNet/GC Cloud enables connectivity between 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 EFCD user access requires two-factor authentication. A certificate (token or smart card) and password is required for authenticating users that access RTID.

2. EFCD users directly connecting to RTID must establish a secure VPN using two-factor authentication. Once established the EFCD will be able to send/receive compliant NIST packets to/from RTID. The EFCDs must support establishing a secure connection and communicating with RTID to support all the requirements throughout the SOR and its accompanying documents.

3. For permanently established secure VPNs, EFCD/SMTP-SPOI devices must operate within the secure tunnel created to support all the requirements throughout the SOR and its accompanying documents. The RCMP/GC/CPMG will be responsible for establishing permanent secure VPNs.

2.3 Current High-Level RCMP/GC/CPMG Architecture

1. Figure 2-2: Current RTID High-Level Architecture, depicts the EFCD/SMTP-SPOI connectivity within the RCMP/GC/CPMG architecture. It is presented herein to show the relationship between the RCMP/SSC conceptual security architecture, the RTID components and the EFCD/SMTP-SPOI devices.

2. A brief description of each component was provided in the Appendix A SOR. More detailed descriptions of the components are included in Section 3 New EFCD and SPOI detailed Architecture.

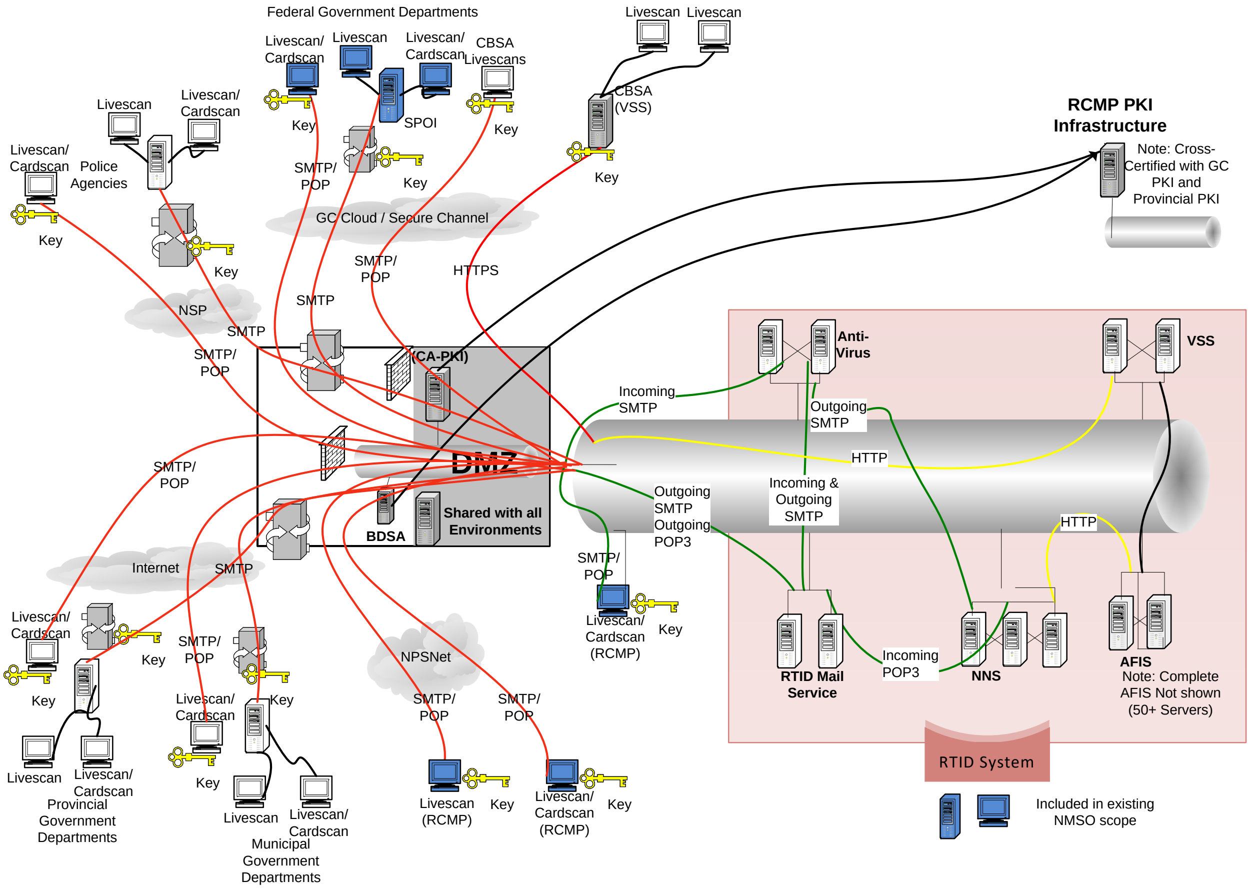

Figure 2-2: Current RTID High-Level Architecture

3. NEW EFCD AND SPOI SCOPE WITHIN CURRENT ARCHITECTURE

3.1 Example EFCD and SPOI Connectivity Architecture

1. The following diagram, Figure 3-1: Example EFCD / SPOI Connectivity Architecture, depicts example EFCD and SPOI connectivity. The diagram depicts various combinations of devices within the architecture to show the common connectivity options between the EFCD/SPOI devices and other devices within the RTID architecture.

2. A Livescan or Cardscan can directly connect to RTID by establishing a secure encrypted connection. Once established, assuming the operator has a valid certificate that allows them to connect to RTID, the EFCD will be able to communicate with RTID using SMTP and POP.

3. Multiple EFCDs can connect to a SPOI and the SPOI will directly connect to RTID through a secure encrypted connection. The SPOI will support communicating with RTID using bi-directional SMTP as well as communicating the results from the RTID to the appropriate EFCD. The communication to/from an NMSO EFCD to the SPOI is SMTP/POP. An alternate communication protocol may be acceptable to the RCMP/GC/CPMG; however, it must satisfy the RTID/RCMP security requirements and must be approved by the RCMP/GC/CPMG.

4. An EFCD can also send/receive between an RMS/DMS using SMTP and/or POP. For example, information related to an individual that is being fingerprinted can be provided by the RMS to the EFCD, which the EFCD will use to create NPS-NIST compliant packets that will be sent to RTID. The detailed requirements for this communication between the EFCDs and an RMS/DMS are described in Annex B to Appendix A – EFCD Detailed Requirements.

5. An EFCD can also request data regarding an individual being fingerprinted from a department/agency system to obtain data that will be automatically populated into the appropriate fields in the EFCD UI and NPS-NIST packet as required. CBSA is used as an example in Figure 3-1: Example EFCD / SPOI Connectivity Architecture to depict this connectivity using HTTP. The detailed requirements for this communication between the EFCDs and the department/agency system are described in Annex B to Appendix A – EFCD Detailed Requirements.

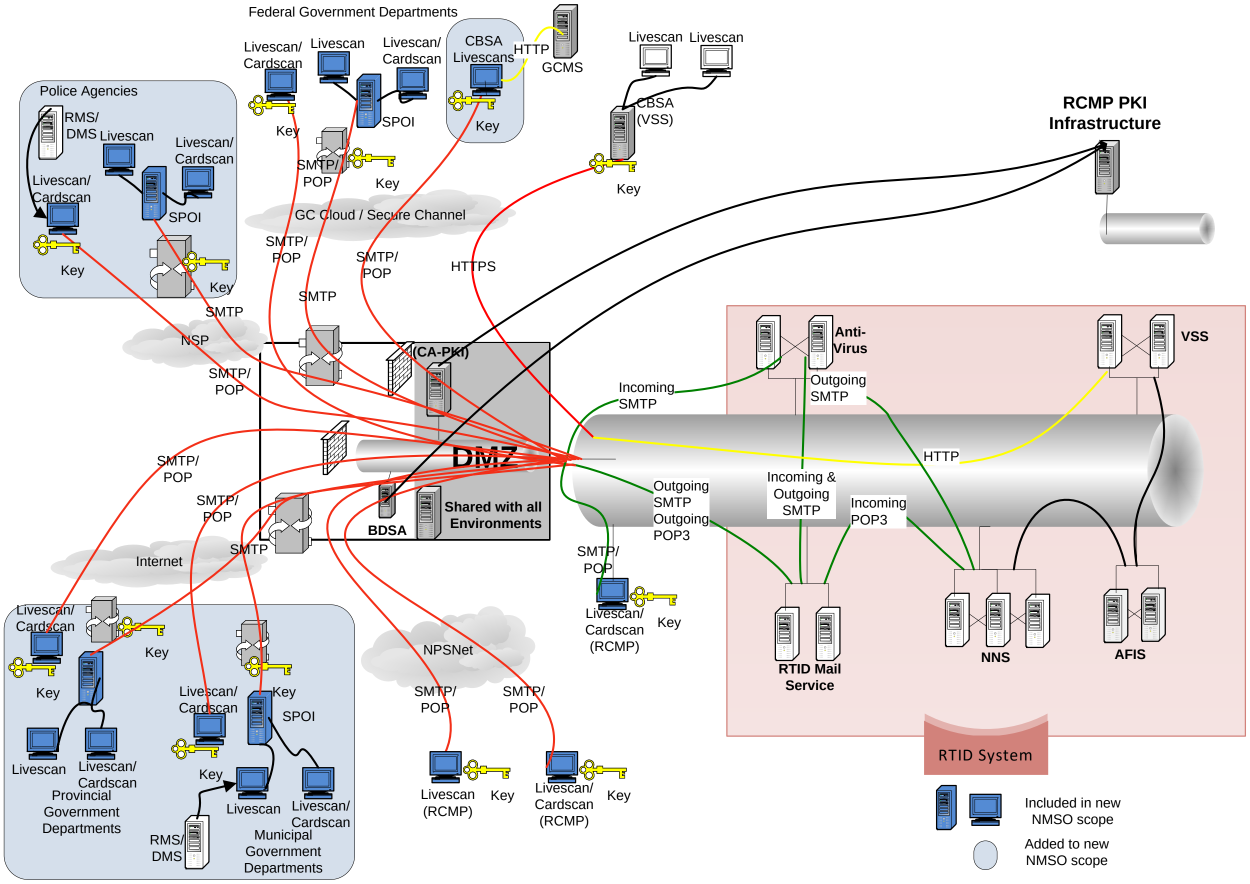

Figure 3-1: Example EFCD / SPOI Connectivity Architecture

3.2 Example Detailed EFCD and SPOI Site Connectivity

1. Figure 3-2: Example EFCD / SPOI Site Connectivity depicts various types of EFCDs, SPOI and peripherals configured at a site. This detailed diagram shows an example of how multiple EFCDs could be connected at a site with a SPOI used to communicate to RTID.

2. Figure 3-3: Example Single Kiosk Livescan Site Connectivity depicts a single Kiosk Livescan establishing a secure connection from the Kiosk to RTID through GC Cloud.

3. Figure 3-4: Example Single Desktop Livescan Site Connectivity depicts a single Desktop Livescan establishing a secure connection from the Livescan to RTID through the Internet.

4. All of these examples depict a common security architecture where any device must use an existing secure connection or establish a secure connection to RTID before any communication can be completed. When a SPOI is used, it is the agency's responsibility to ensure all communication to/from the EFCDs and the SPOI is appropriately secure to satisfy RTID requirements.

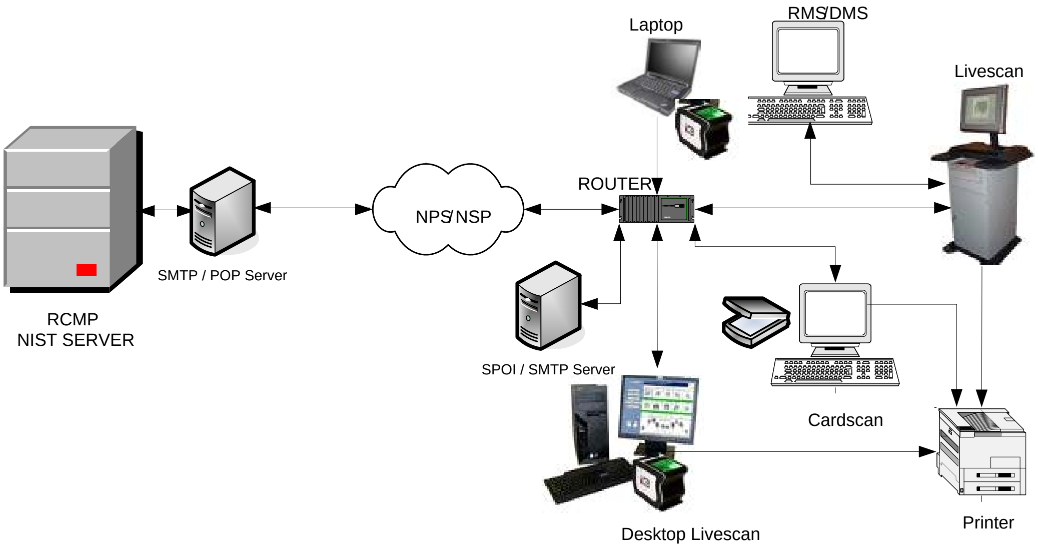

Figure 3-2: Example EFCD / SPOI Site Connectivity

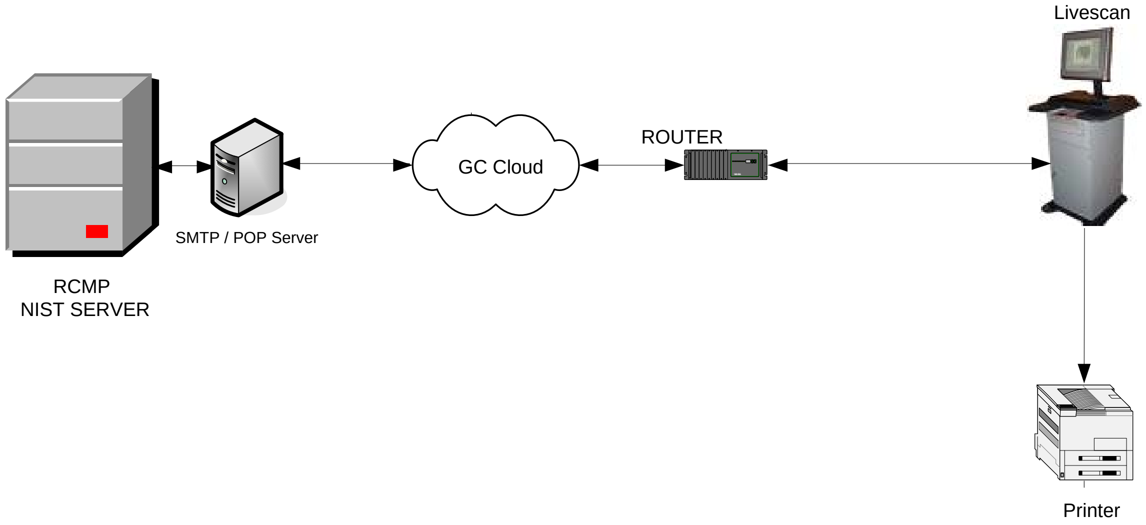

Figure 3-3: Example Single Kiosk Livescan Site Connectivity

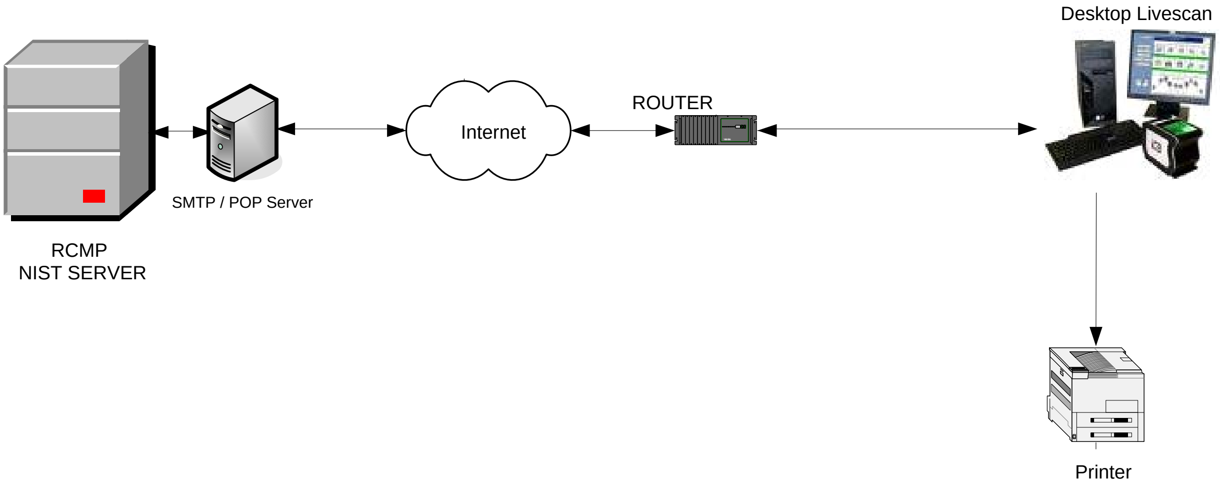

Figure 3-4: Example Single Desktop Livescan Site Connectivity