Architecture

Microsoft Dynamics CRM 4.0

Connectivity and Firewall Port Requirements in On-Premise Deployments

White Paper: "Nuts and Bolts" Series
Security and Authentication in Microsoft Dynamics CRM

Practical Application

Date: January 2010

Microsoft Dynamics

Acknowledgements

Initiated by the Microsoft Dynamics CRM *Engineering for Enterprise* (MS CRM E^2) Team, this document was developed with support from across the organization and in direct collaboration with the following:

Key Contributors

Peter Simons (*Microsoft*)
Roger Gilchrist (*Microsoft*)

Technical Reviewers

Mahesh Hariharan (*Microsoft*)
Monika Borgaonkar (*Microsoft*)
Greg Kilponen (*Microsoft*)

The MS CRM E^2 Team recognizes their efforts in helping to ensure delivery of an accurate and comprehensive technical resource in support of the broader CRM community.

MS CRM E^2 Contributors

Amir Jafri, Program Manager
Jim Toland, Content Project Manager

Feedback

Please send comments or suggestions about this document to the MS CRM E^2 Team feedback alias (entfeed@microsoft.com).

Microsoft Dynamics is a line of integrated, adaptable business management solutions that enables you and your people to make business decisions with greater confidence. Microsoft Dynamics works like and with familiar Microsoft software, automating and streamlining financial, customer relationship and supply chain processes in a way that helps you drive business success.

U.S. and Canada Toll Free 1-888-477-7989
Worldwide +1-701-281-6500
www.microsoft.com/dynamics

Legal Notice

Table of Contents

Preface

CRM E^2 Nuts and Bolts Series Overview

The MS CRM Engineering for Enterprise (E^2) *Nuts and Bolts* (NB) series is an expanding set of topical content, with each offering providing detailed information about the internal mechanisms related to a specific area of functionality within Microsoft Dynamics CRM 4.0.

NB Series offerings are designed to provide detailed technical resources that:

- Address often repeated queries to technical aliases
- Consolidate answers, links, etc., that are generated in response to those queries
- Offer multiple levels of complementary information to support a broader, multi-perspective understanding of the topic
- Convey the baseline "principles" users require to begin to address related but tangential technical queries
- Present content using a consistent structure and "look and feel"

Audience

The target audience of the NB Series includes (but is not limited to):

- Solution Architects
- Application Architects
- Infrastructure Architects
- Consultants
- Developers

NB Article Content and Structure

Articles in the NB Series are designed to accommodate information at three independent but complementary levels (or "tiers"), which are shown in the following table:

Tier	Description
Core Architecture	High-level, architectural information; "schematic-level " view of functionality; provides contextual overview/baseline knowledge
Conceptual Application	Best practices and guidelines associated with CRM features or functionality that can be applied based on the specifics of particular implementation
Practical Application	Detailed explanations about how to address unique scenarios; practical details about resolving issues or accomplishing specific "real-world" tasks

This component of the Nuts and Bolts article *Security and Authentication in Microsoft Dynamics CRM* addresses selected aspects of the practical application of the Microsoft Dynamics CRM 4.0 security model.

The full breadth of coverage provided by the Nuts and Bolts article *Security and Authentication in Microsoft Dynamics CRM* includes the following:

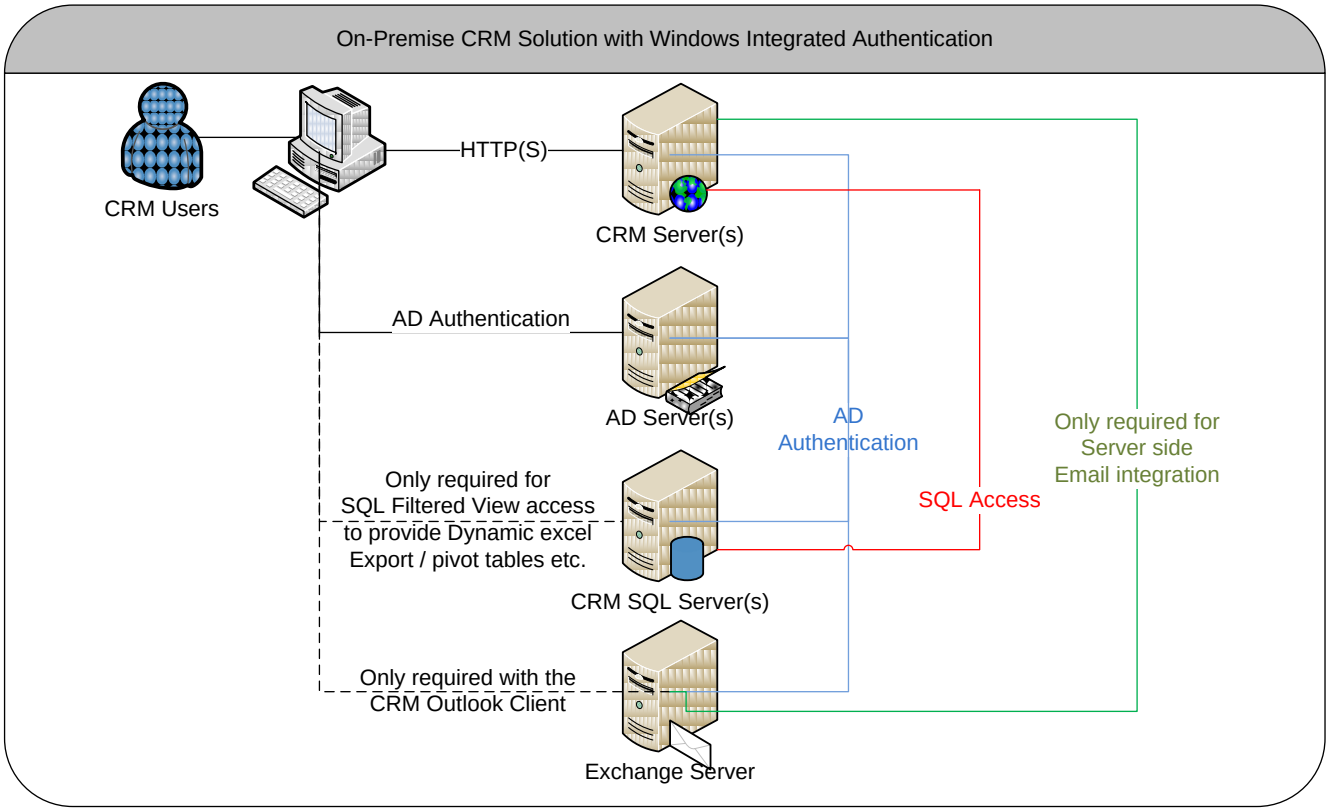
- Core Architecture
  - *The Microsoft Dynamics CRM Security Model*
- Conceptual Application
  - *Securing Microsoft Dynamics CRM in the Enterprise*
  - *Field-level Security in Microsoft Dynamics CRM: Options and Constraints*
  - *Securing the Network Infrastructure for Microsoft Dynamics CRM*
- Practical Application
  - *Security Contexts in Microsoft Dynamics CRM*
  - *Connectivity and Firewall Port Requirements in On-Premise Deployments*

Overview

Many data centers include firewalls between the end-users and the servers and other integrated systems that support an implementation of Microsoft Dynamics CRM 4.0. This document is designed to provide guidance on the connectivity requirements between Microsoft Dynamics CRM 4.0 and other systems to assist readers with proper firewall configuration in customer environments.

On Premise with Integrated Windows Authentication

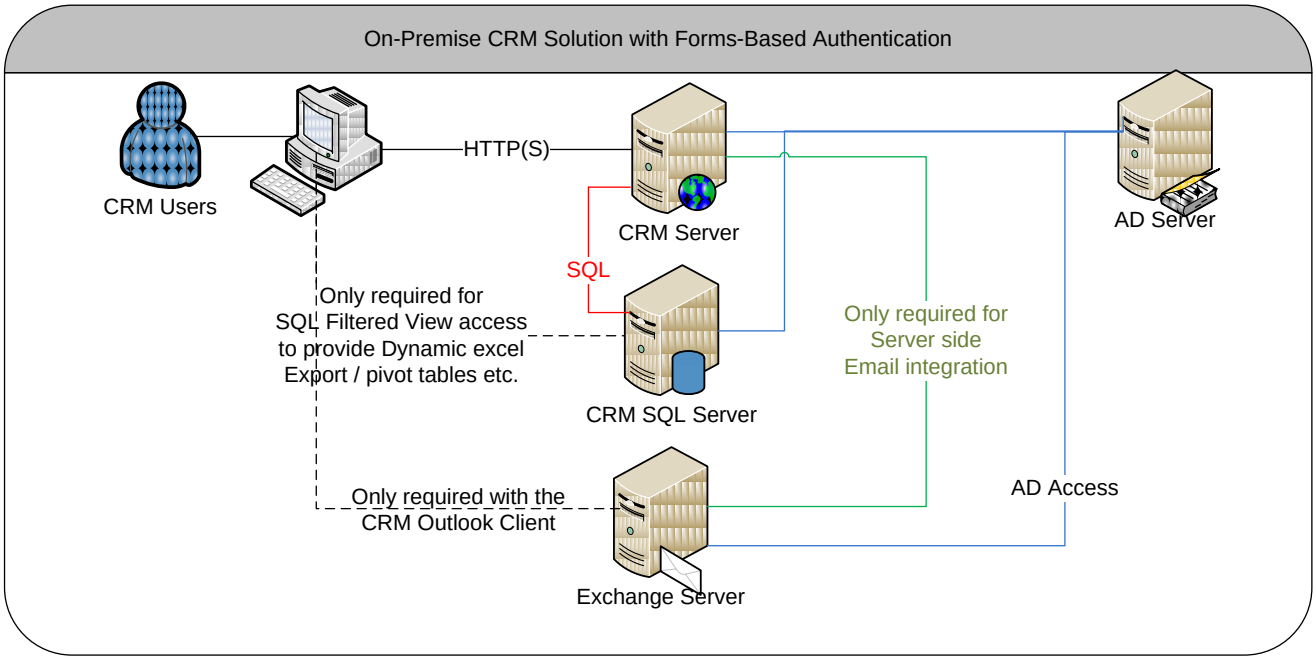
An overview of an on-premise implementation that uses Integrated Windows Authentication (IWA) is shown in the following diagram:



In this scenario the user must have a certain level of connectivity to the CRM Server(s), the Active Directory Server(s) and the SQL Server for SQL Filtered View access (if Export to Excel functionality is required). The remainder of this document focuses primarily on this scenario and details the required level of connectivity between these various components as well as further options for integration, Citrix implication etc.

On Premise with Forms-Based Authentication

An overview of an on-premise implementation that uses forms-based authentication using an Internet Facing Deployment (IFD) configuration is shown in the following diagram:



In IFD, the web site is accessed anonymously and is then redirected to a sign in aspx page. This page then authenticates the user against a back office AD Server and generates a CRM ticket cookie for the session. If the session cookie times out or a request is sent without the cookie then the user is returned to the sign in page to re-enter their credentials.

By enabling the IFD configuration the user does not require AD connectivity in order to access CRM. They do however still require an AD account. CRM then authenticates the user against AD before granting the CRM ticket cookie.

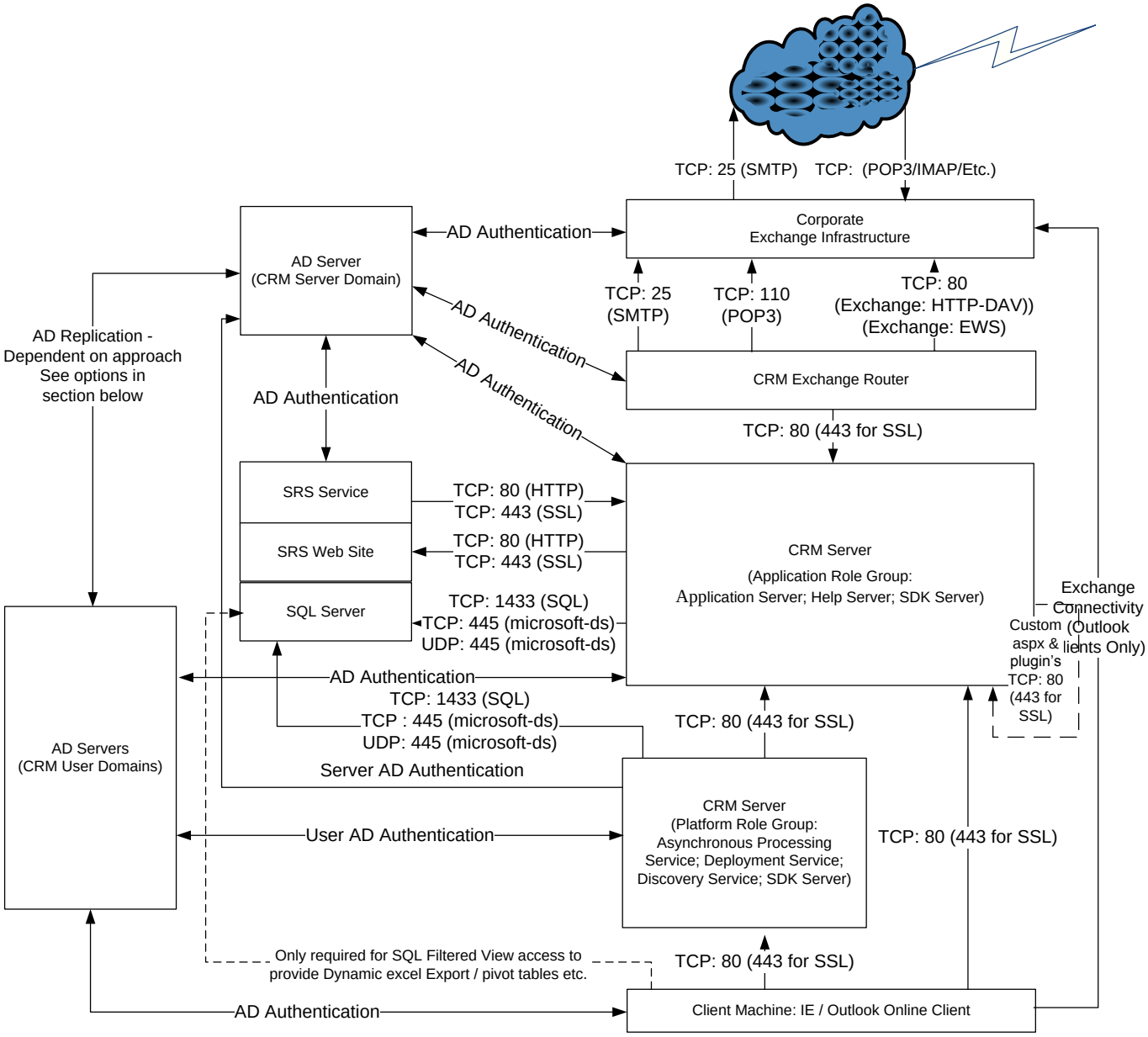
Access to the SQL Server is still required for certain features, such as dynamic excel views and pivot tables, that require direct access to the filtered views.

Note that when using dynamic Excel sheets, one can avoid direct access to the SQL Server by using the Registry key "UseWebQueryForLiveExport" to ensure that dynamic Excel sheets use the FetchXML route. This Registry key is particularly handy when an Excel sheet is accessing a Internet facing CRM deployment from outside the AD network.

Note: For more information about avoiding direct access to the SQL Server when using dynamic Excel sheets, on the CRM Blog, see the article *Dynamic Export to Excel feature – How to protect data over the wire* at:
http://blogs.msdn.com/crm/archive/2009/01/26/dynamic-export-to-excel-feature-how-to-protect-data-over-the-wire.aspx"

Default CRM Connectivity Requirements

AN overview of the default connectivity requirements for an on-premise deployment of Microsoft Dynamics CRM 4.0 is shown in the following graphic:



In addition all Servers require the following:

- DNS name resolution on UDP/TCP: 53
- NetBIOS name resolution on TCP: 139, UDP: 137/138
- NTP time synchronisation: 123 – *this is a requirement for Kerberos Authentication*
- DCOM and RPC: TCP 135, UDP 1025

***Note**. Arrow direction depicts source and target of initiating request rather than direction of data flow*

Important: Because this diagram is focused on CRM connectivity requirements, full details about the specific port requirements for Microsoft Exchange Server and the Microsoft Windows Active Directory® service are not shown. Additional information and links to related articles about these technologies and their specific requirements are provided in the following sections of this document.

The default connectivity requirements for components of an on-premise deployment of Microsoft Dynamics CRM 4.0 are shown in the following table:

Component	Default Connectivity Requirements
CRM Server	▪ AD Connectivity from CRM Servers ▪ RDP Connection to all Servers recommended ▪ SQL Server access ▪ SQL Reporting Services access
Exchange Router	▪ Exchange Server Connectivity (HTTP DAV / EWS* / STMP) ▪ Other Mail Server Connectivity (POP3/SMTP) ▪ Optional Connectivity to a CRM Sink Mailbox ▪ HTTP / HTTPS access to CRM Servers / Network Load Balancer ▪ AD Authentication
Client	▪ Outlook Connectivity to Exchange ▪ Optional Connectivity to SQL Server for views ▪ HTTP / HTTPS access to CRM Servers / Network Load Balancer ▪ AD Authentication
ALL	▪ DNS name resolution where applicable on UDP/TCP: 53 ▪ NetBIOS name resolution where applicable on TCP: 139, UDP: 137/138 ▪ NTP: Required on all Servers to Sync Network Time UDP: 123 – *this is a requirement for Kerberos Authentication* ▪ DCOM and RPC: Required on all Servers. TCP 135, UDP 1025

** Exchange Web Services (EWS) Introduced in CRM 4.0 UR8 and R4 in Live to support Exchange 2010 and Exchange Online*

Important: In each case, the port numbers can be configured to run under alternative (non-default) values, so environments will vary.

Port Recommendations for CRM and SQL Servers

The port recommendations for CRM Servers and SQL Servers, which are provided in the *Microsoft Dynamics CRM 4.0 Implementation Guide*, are shown in the following tables.

CRM Servers

Protocol	Port	Description	Explanation
TCP	80	HTTP	Default Web application port; may be different as it can be changed during Microsoft Dynamics CRM Setup. For new Web sites, the default port number is 5555
TCP	135	MSRPC	RPC endpoint resolution
TCP	139	NETBIOS-SSN	NETBIOS session service
TCP	443	HTTPS	Default secure HTTP port; may vary from the default port. This secure network transport must be manually configured. Although this port is not required to run Microsoft Dynamics CRM, it is strongly recommended. **Note:** For information about how to configure HTTPS for Microsoft Dynamics CRM, in the *Implementation Guide*, see the topic "Make Microsoft Dynamics CRM 4.0 client-to-server network communications more secure."
TCP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication.
UDP	123	NTP	Network Time Protocol
UDP	137	NETBIOS-NS	NETBIOS name service
UDP	138	NETBIOS-dgm	NETBIOS datagram service
UDP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication
UDP	1025	Blackjack	DCOM, used as an RPC listener

SQL Servers running the CRM Connector for SQL Reporting Services

Protocol	Port	Description	Explanation
TCP	135	MSRPC	RPC endpoint resolution.
TCP	139	NETBIOS-SSN	NETBIOS session service.
TCP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication.
TCP	1433	ms-sql-s	SQL Server sockets service; required for access to SQL Server; this number may vary if you have configured your SQL Server to use a different port number.
UDP	123	NTP	Network Time Protocol
UDP	137	NETBIOS-NS	NETBIOS name service
UDP	138	NETBIOS-dgm	NETBIOS datagram service
UDP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication
UDP	1025	Blackjack	DCOM, used as an RPC listener

Connectivity Requirements for Windows Services

Microsoft client, server, and server-based programs use a variety of network ports and protocols to communicate with client systems and with other server systems over the network.

While beyond the scope of this article, details of the essential network ports, protocols and services that are used by Microsoft client and server operating systems, server-based programs, and their subcomponents in the Microsoft Windows server system are available in Microsoft Help and Support, in the article *Service overview and network port requirements for the Windows Server system* at http://support.microsoft.com/kb/832017

Connectivity Requirements for Integrated Windows Authentication

The key service and port requirements for Integrated Windows Authentication (IWA) are shown in the following table:

Service Name	UPD	TCP
LDAP	389	389
LDAP SSL	N/A	636
RPC Endpoint Mapper	135	135
Global Catalog LDAP	N/A	3268
Global Catalog LDAP SSL	N/A	3269
Kerberos	88	88

However, in larger deployments, firewalls can present two challenges when deploying a distributed Active Directory (AD) directory service architecture:

- Initially promoting a server to a domain controller
- Replicating traffic between domain controllers

Active Directory relies on remote procedure call (RPC) for replication between domain controllers. Note that while Simple Mail Transfer Protocol [SMTP] can be used in certain situations—schema, configuration, and global catalog replication—but not domain naming context, which limits its usefulness.

Configuring replication in environments in which a directory forest is distributed among internal, perimeter networks and external (that is, Internet-facing) networks can be challenging. In these scenarios, there are three possible approaches:

- Open the firewall wide to permit RPC's native dynamic behavior
- Limit RPC's use of TCP ports and open the firewall just a little bit
- Encapsulate domain controller (DC-to-DC) traffic inside IP Security Protocol (IPSec) and open the firewall for that

Each approach has its pros and cons; in general, there are more cons than pros associated with the entry at the top of the list, and more pros than cons associated with the entry at the bottom of the list.

Note: For more information about each option, including details of the configuration and ports requirements for each, on Microsoft TechNet, see *Active Directory Replication over Firewalls* at http://technet.microsoft.com/en-us/library/bb727063.aspx.

Mail Server Connectivity Requirements

Microsoft Dynamics CRM 4.0 provides for integration with Exchange and other SMTP/POP3 servers. Mail system integration is typically achieved either through client-side integration via Outlook or server-side integration via Exchange or other third-party SMTP / POP3 server

Note: This document focuses on server-side integration via Exchange, but the same principles would apply to server-side integration via other POP3/SMTP servers.

Administrators can specify to use either client side / server side integration, which can be configured at a user level within the User properties in CRM. After the administrator specifies the level at which integration will occur, users on the client computers must agree to have email sent on their behalf by CRM by using their own user options configuration.

While client-side integration does not require any additional server components, it works only with the CRM Outlook clients. The Outlook client plug-in is then used to send email via Outlook and the users' preconfigured mail Server as well as to route inbound emails back into CRM. This integration happens on a regular polling basis (but is not immediate). Additional CRM specific ports are not required for this integration; standard Exchange connectivity is used. Emails are routed into CRM via the CRM Web Services; hence access to Port 80 (443 for SSL) from the Outlook Client is the only requirement.

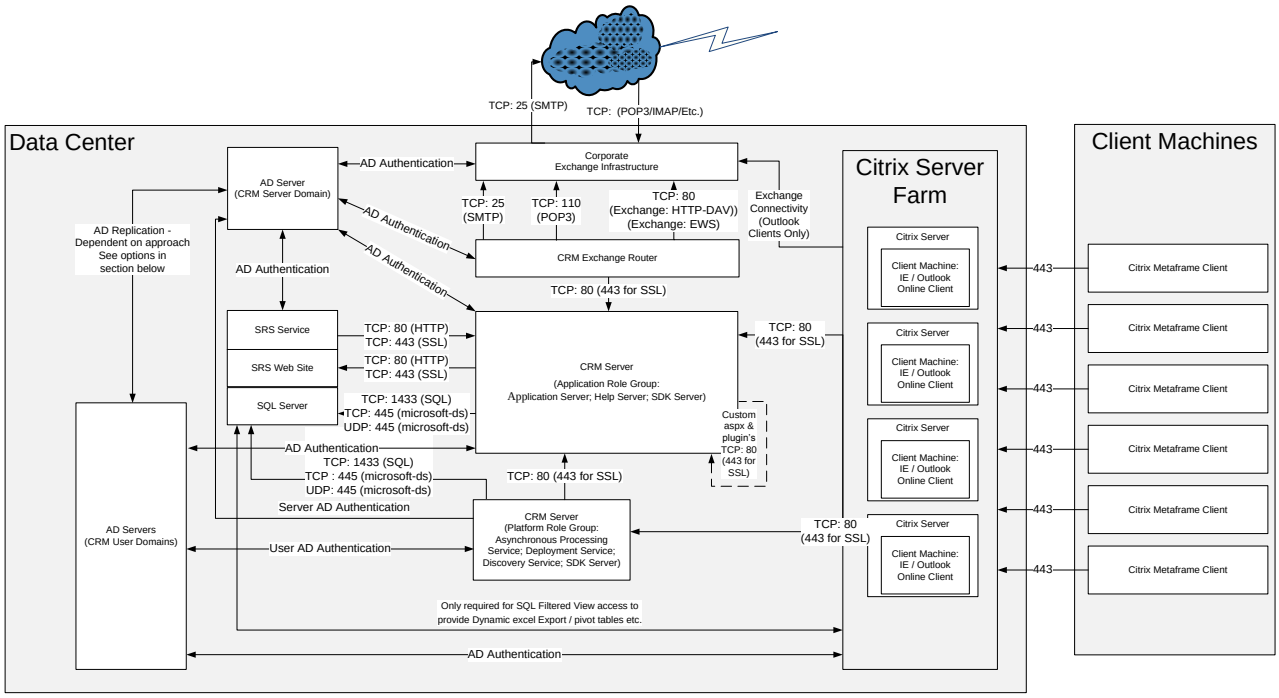
The CRM Exchange Router can be installed on an Exchange Server or on a dedicated CRM Exchange Router server. Using the CRM Exchange Router provides inbound and outbound email connectivity for both the CRM Web client and CRM Outlook clients. This CRM Exchange Router integrates with external mail systems via:

- POP3 (TCP:110) and SMTP (TCP:25)
- HTTP-DAV (TCP:80) for the CRM Sink account or direct to users mail account
- Exchange Web Service (EWS) (TCP:80)

Citrix Server Implications

Citrix Presentation Servers have the same connectivity requirements as those discussed previously for CRM Clients. In addition, users must be able to connect to the Citrix Servers on the predefined Citrix port. The default Citrix access via Citrix Secure Gateway or the SSL Relay service for Citrix ICA connections only requires TCP port 443.

The diagram below shows how a Citrix Server Farm can simplify the connectivity requirements in a complex environment:



In addition all Servers require the following:

- DNS name resolution on UDP/TCP: 53
- NetBIOS name resolution on TCP: 139, UDP: 137/138
- NTP time synchronisation: 123 – *this is a requirement for Kerberos Authentication*
- DCOM and RPC: TCP 135, UDP 1025

Only required for SQL Filtered View access to provide Dynamic excel Export / pivot tables etc.

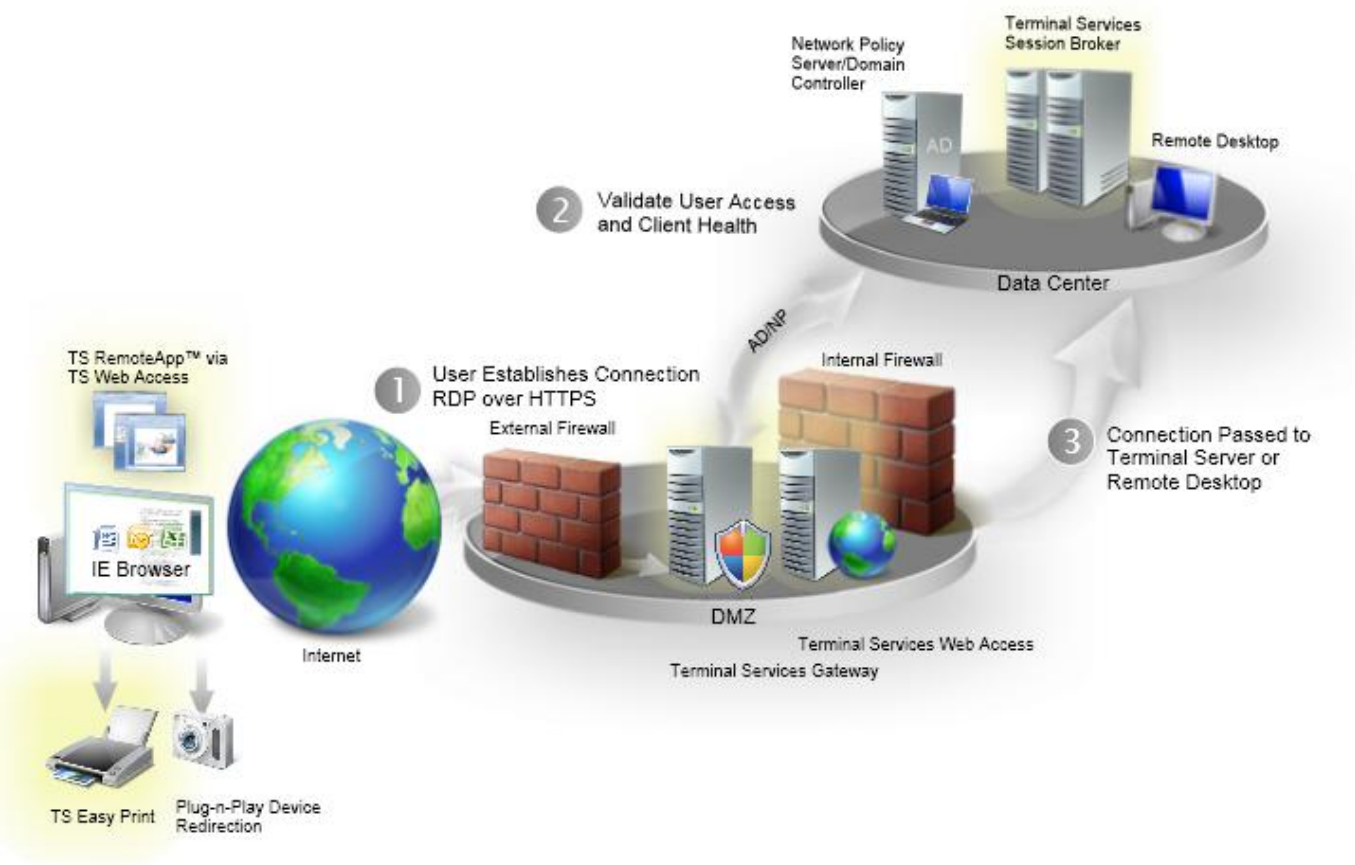
***Note**. Arrow direction depicts source and target of initiating request rather than direction of data flow*

The primary considerations with a Citrix deployment are:

- If you are going to host the full users desktop on Citrix then this can lead to the need for a very large server farm to provide the required resources. Hosting the users Outlook experience from a Citrix deployment can degrade the user experience and removes the ability for the user to work offline. In the event of a network failure they will have no capability to use any of the functionality provided from the Citrix farm.
- If you already host the full users experience out of Citrix then it should be noted that CRM will require significantly more resources per user. The primary increase is in terms of memory where you should allow at least an additional 200MB per concurrent CRM Outlook Client in your Citrix Server farm.
- If you are going to provide access via the CRM Web Client via a Citrix Server then this can provide improved performance over high latency connections and reduce the need for firewall changes. This is the most frequently used approach for combining Citrix and Microsoft Dynamics CRM 4.0. In this case you should allow for 100MB of memory per concurrent CRM Web Client user.

Microsoft Presentation Virtualization using Windows Server 2008 Terminal Services

Microsoft can provide the same benefits found with Citrix implementations using the Windows Server 2008 Terminal Services – Presentation Virtualization. In this scenario, Microsoft Terminal Services Gateway can be used to establish a secure RDP session over an SSL tunnel, or Terminal Services Web Access can provide terminal services access from an IE browser over an SSL connection.



Note: For additional information on the options available with Microsoft Presentation Virtualization, on the Windows Server 2008 R2 site, see *Remote Desktop Services* a: http://www.microsoft.com/windowsserver2008/en/us/ts-product-home.aspx

Appendix A: Resources

For additional information related to connectivity and firewall port requirements in Microsoft Dynamics CRM 4.0, see the following additional resources:

- *Microsoft Dynamics CRM 4.0 Implementation Guide*
  http://www.microsoft.com/downloads/details.aspx?FamilyId=1CEB5E01-DE9F-48C0-8CE2-51633EBF4714&displaylang=en
- *Service overview and network port requirements for the Windows Server system*
  http://support.microsoft.com/kb/832017
- *Securing Your Application Server*
  http://msdn.microsoft.com/en-us/library/aa302433.aspx