MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback by Matrix42

How to protect your Exchange environment

Version 1.0

27. February 2015

Copyright © 2000 - 2014 Matrix42 AG

This documentation is copyright protected. All rights are reserved by Matrix42 AG.

Any other use, in particular the disclosure to third parties, storage in a data system, dissemination, processing, presentation, performance and demonstration are prohibited. This applies to the entire document, as well as parts thereof.

Subject to change. Reprint, also in excerpts, is permitted only with the written consent of Matrix42 AG.

The software described in this document is subject to a permanent development due to which there may be differences in the documentation and the actual software. This documentation is not entitled to the actual functionality of the software.

Apple and **Mac OS X** are registered trademarks of Apple Inc.
Citrix® software or **Citrix® server** are Trademarks and Registered Trademarks of Citrix Systems, Inc. in the United States and other countries.
cygwin is copyrighted by Red Hat Inc. 1996-2003.
expat is copyrighted by Thai Open Source Software Center Ltd.
gSOAP is copyrighted by Robert A. van Engelen, Genivia, Inc. All rights reserved.
Iconv is copyrighted by 1999-2003 Free Software Foundation, Inc.
Iperf is copyrighted by the University of Illinois, except for the gnu_getopt.c, gnu_getopt_long.c, gnu_getopt.h files, and inet_aton.c, which are under the GNU General Public License.
Libmspack (C) 2003-2004 by Stuart Caie <kyzer@4u.net>.
OpenSSL This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
PuTTY is copyrighted by Simon Tatham. Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, and CORE SDI S.A.
RSA Data Security, Inc. MD5 Message-Digest Algorithm is copyrighted by RSA Data Security Inc. Created 1991. All rights reserved.
rsync is an open source utility that provides fast incremental file transfer. rsync is freely available under the GNU General Public License version 2.
runcontrol The Initial Developer of the Original Code is James Clark. Portions created by James Clark are Copyright (c) 1998 James Clark. All rights reserved.
SNMP++ Copyright (c) 1996 Hewlett-Packard Company.
VMware, the **VMware "boxes" logo and design, Virtual SMP, VMotion vSphere, vSphere Hypervisor (ESXi), ESX, View, ThinApp, vCenter** and **vCloud** are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
Windows, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, **Windows Server 2012,** and **Microsoft Exchange** are registered trademarks of Microsoft Corporation.

Others, at this point not explicitly listed, company, brand and product names are trademarks or registered trademarks of their respective owners and are subject to trademark protection.

Contents

1. Introduction 4
2. Architecture 5
3. Authentication 6
3.1. Basic Authentication with PowerShell Integration 7
3.1.1. Basic Authentication with PowerShell Network Overview 8
3.2. Pass-through Authentication with PowerShell Integration 9
3.2.1. Pass-through Authentication with PowerShell Network Overview 10
3.3. Enterprise Certificate Authentication 11
3.3.1. Enterprise Certificate Network Overview 12
3.4. Client Certificate Authentication with Kerberos 13
3.4.1. Client Certificate with Kerberos Network Overview 14
4. Conclusion 15

How to protect your Exchange environment

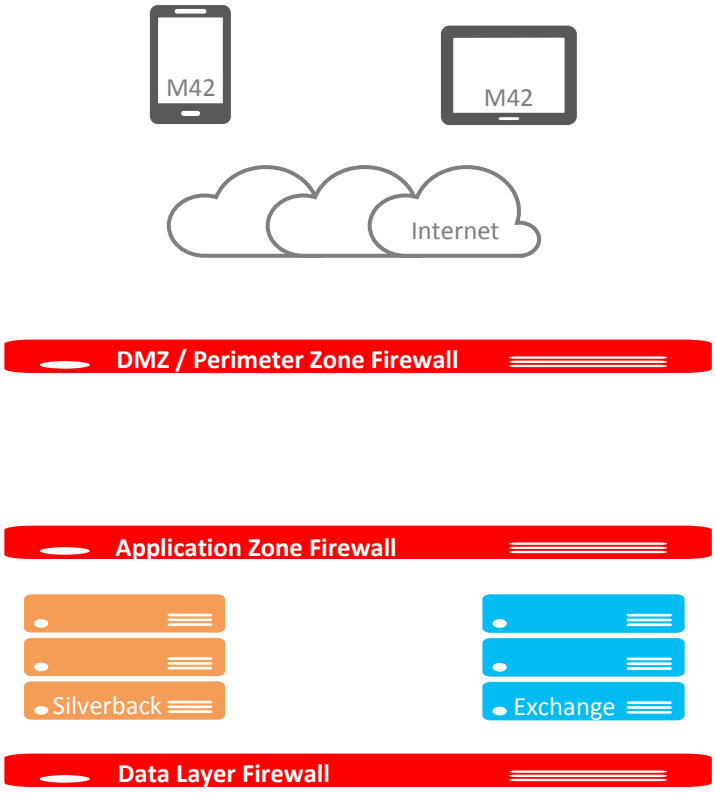
1. Introduction

This guide will help you decide how to control access to you Exchange environment. This allows you to control who can access Exchange ActiveSync from Smartphones and Tablets. Silverback acts as the management platform providing access control over Exchange ActiveSync, based on its policies. Silverback either allows managed devices, or denies unmanaged devices, ensuring a base level of compliance. This is a typical Exchange ActiveSync control mechanism. It leverages the firewall technology decisions you have already made. This means you do not need to install additional firewalls, gateways, reverse proxies or application delivery controllers. This is the most cost effective way to protect exchange, ensuing a greater return on investment for your existing hardware.

2. Architecture

You need to decide what architecture you want to use. Most modern security frameworks suggest a layered architecture. Enterprises need a layered security framework to defend against cyber-attacks.

This provides many layers of security to protect your internal resources. It is important; not only to protect your network but also to ensure all the connecting devices are in compliance with your corporate policy. There are many different architectural patterns that can be chosen, but we will concentrate on the standard perimeter model. This consists of a Perimeter Layer, an Application Layer and a Data Layer. The Perimeter Network can also be referred to by the military term DMZ.



In this architecture, your existing firewall, application delivery platform or proxy server processes the Exchange ActiveSync traffic, before being allowed to connect to Exchange. There are several different ways to ensure the connecting smartphones are under management and compliant. These methods are based on the different authentication methods. You may not be able to deploy all of the methods, as each firewall technology has a different feature set. The method you choose may be driven by the firewall technology you use.

3. Authentication

There are five different authentication models to choose from. These methods are either based on passwords or client certificates.

The password based authentication methods, rely on PowerShell integration to control application access. Once the PowerShell connector is implemented, Silverback sends a complete list of managed smartphones to your Exchange environment. If an unmanaged device tries to connect to Exchange, it is rejected, but all managed devices are allowed to connect. Each time a device is enrolled into Silverback it notifies Exchange to allow the Smartphone. Once a device falls out of compliance, or is manually blocked, Silverback notifies Exchange that the devices should no longer be accepted.

When using one of the client certificate methods, you do not need to implement the PowerShell connector. Since Silverback distributes the certificates, management is implied. Therefore you don't need to implement the PowerShell connector, but if you decide you want to have multiple controls, you can implement both. They function independently of each other.

The complexity of the implementations ranges from simple to very hard, so please consider, security, skill level and budget when deciding on a pattern.

How to protect your Exchange environment

3.1. Basic Authentication with PowerShell Integration

Complexity - Moderate Security - Moderate

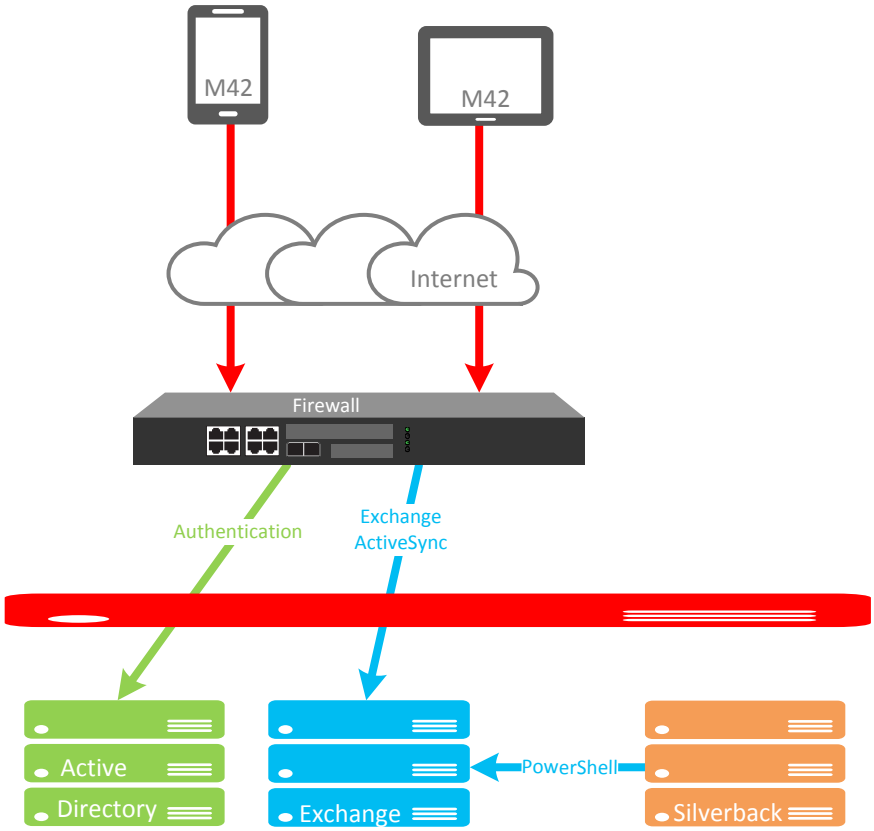
This model authenticates the user in the perimeter network, so the session is authenticated before allowing the traffic to reach the Microsoft Exchange Client Access Servers. This ensures that any malicious activity is restricted to the Perimeter Network.

When a device is enrolled into Silverback, it instructs Exchange to allow that device to connect. The Exchange Server then decides whether the device is allowed to connect.

Most next generation firewalls, load balancers, application delivery platforms and web application firewalls have a web publishing function. These include F5 BigIP, Fortinet Fortigate, Juniper Pulse, Citrix NetScaler Barracuda WAF and many more. Not all firewalls have this feature, so please contact your firewall vendor for specific support.

Configure your firewall to terminate the Exchange ActiveSync TLS traffic, and request basic authentication. The device will use the credentials it has configured in its Silverback MDM Exchange profile, to authenticate with your firewall. Your firewall authenticates these credentials against you internal Domain Controllers. Successfully authenticated users will be allowed through to the Exchange server, and Exchange Quarantine will check whether the smartphone is allowed.

3.1.1. Basic Authentication with PowerShell Network Overview



3.2. Pass-through Authentication with PowerShell Integration

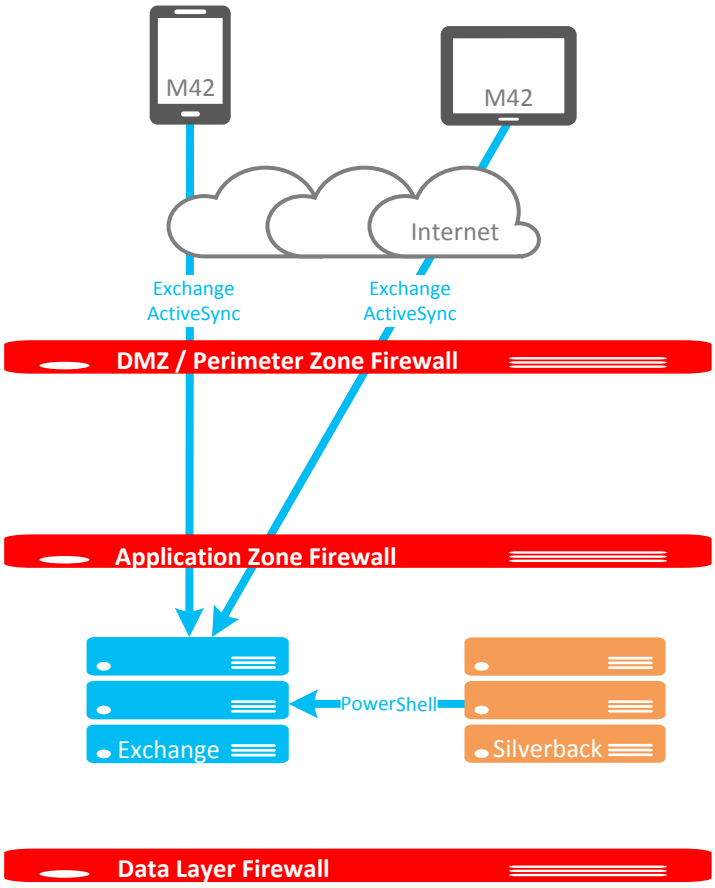
Complexity - Low Security - Basic

This model allows the smartphone to connect through the perimeter network, connecting directly to Exchange. The Exchange CAS Server authenticates the session.

When a device is enrolled into Silverback it instructs Exchange, via Microsoft PowerShell, to authorise that device. The Exchange Server then decides whether a connecting device should be allowed to connect. This removes the necessity to configure your permitter firewall to terminate and process the traffic, but allows Internet traffic to terminate in your Application Layer. This type of perimeter transversal is known as zone hoping and can increase your attack surface. Most security policies deny the use of zone hoping in architectural designs, as it exposes your internal system to external attack.

The device will use the credentials it has configured in its Silverback MDM Exchange profile, to authenticate with your Exchange CAS Servers. Successfully authenticated users will be allowed through to the Exchange server, and Exchange Quarantine will check whether the smartphone is allowed.

3.2.1. Pass-through Authentication with PowerShell Network Overview



3.3. Enterprise Certificate Authentication

Complexity - Moderate | Security - High

This model authenticates the user in the perimeter network, so the session is authenticated before allowing the traffic to reach the Microsoft Exchange Client Access Servers. This ensures that any malicious activity is restricted to the Perimeter Network.

This method is similar to the “Basic Authentication with PowerShell Integration” model, but we are using a common Enterprise Certificate to authenticate.

Most next generation firewalls, load balancers, application delivery platforms and web application firewalls have a web publishing function. These include F5 BigIP, Fortinet Fortigate, Juniper Pulse, Citrix NetScaler Barracuda WAF and many more. Not all firewalls have this feature, so please contact your firewall vendor for specific support.

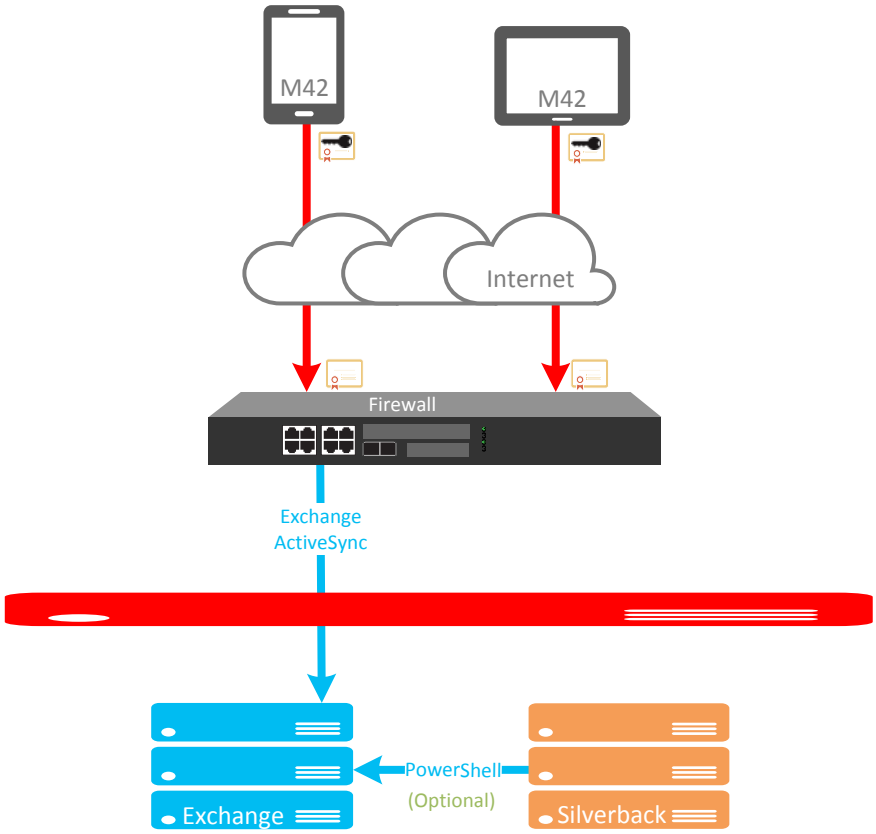
Configure your firewall to terminate the Exchange ActiveSync TLS traffic, and require client certificate authentication. You will need to set the Certificate Trust List, to only allow authentication from the Certificate Authority that generated the enterprise certificate. If your Public Key Infrastructure has multiple layers, please make sure you have the correct certificate Trusted Root and Intermediate CA certificates configured in the chain.

Your Smartphones will use the enterprise certificate configured in their Silverback MDM Exchange profiles, to authenticate with your firewall. Once your firewall correctly authenticates the client certificates against the Certificate Trust List, the connection will be allowed through to the Exchange server. Exchange access will be authorised using the username and password (Basic Authentication) in the Silverback MDM Exchange profile.

If you enable PowerShell integration configured as an additional measure, the Exchange Quarantine will also check whether the smartphone is allowed.

This model may be suitable if you have a strict 2-factor authentication security policy. Something you have “Client Certificate”, something you know “Password”.

3.3.1. Enterprise Certificate Network Overview



3.4. Client Certificate Authentication with Kerberos

Complexity – Very High | Security – Very High

This model is the most secure way to deploy Exchange ActiveSync and is appropriate for companies that require a strong security posture and take security seriously. This architecture has a reduced attack surface and is resilient against most known man-in-the-middle attacks. It mitigates any external brute force attack, password guessing and a range of Distributed Denial of Service attacks. This model doesn't use passwords so the users cannot lock themselves out, so this model is relevant for companies that have a substantial account lockout issue.

This model authenticates users in the perimeter network, so the sessions are authorised before allowing the traffic to reach the Microsoft Exchange Client Access Servers. This ensures that any malicious activity is restricted to the Perimeter Network.

This functionality is only available on a small number of firewalls and application delivery platforms. These include F5 BigIP, Microsoft TMG, Fortinet Fortigate, Juniper Pulse and Citrix NetScaler. Not all firewalls have this feature, so please contact your firewall vendor for specific support.

Configure your firewall to terminate the Exchange ActiveSync TLS traffic and request client certificate authentication. You will need to set the Certificate Trust List to only allow authentication from the Certificate Authority used to generate your individual user certificates. If your Public Key Infrastructure has multiple layers, please make sure you have the correct Trusted Root certificate and Intermediate certificates configured in the chain.

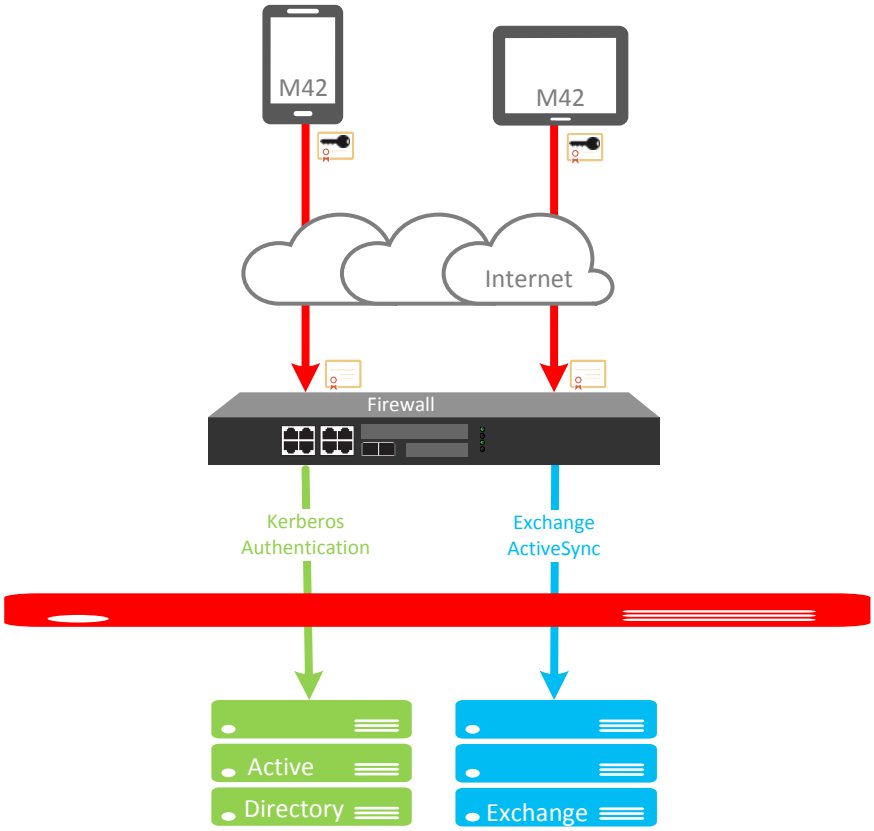
Each Smartphone will use the individual client certificate configured in its Silverback MDM Exchange profiles to authenticate with your firewall. Your firewall will authenticate these credentials against its Certificate Trust List. Since no passwords are used, the firewall will need to perform Kerberos Protocol Transition (KPT) to convert the Client Certificates into Kerberos Tickets. If we don't have a password, then we can't use basic authentication.

You will need to configure your firewall to act as a proxy for Kerberos Constrained Delegation (KCD), so it can requests tickets from a Domain Controller (DC) or Key Distribution Center (KDC). These Kerberos tickets are added to the Exchange traffic.

Successfully authenticated users will be allowed to access the Exchange server, and they now get authenticated using Windows Authentication.

In this kind of model it is not recommended to use PowerShell integration because it is an unnecessary performance hit.

3.4.1. Client Certificate with Kerberos Network Overview



4. Conclusion

Each of the different models has their advantages and disadvantages. The perfect fit for each customer will depend on the size, industry vertical and security posture. This table will help to evaluate each option:

Model	Complexity	Security
Basic Authentication with PowerShell	Moderate	Moderate
Pass-through Authentication with PowerShell	Low	Basic
Enterprise Certificate Authentication	Moderate	High
Client Certificate Authentication with Kerberos	Very High	Very High

Fast deployment for small or pilot customers

If you need to deploy an Exchange control quickly without having to make many changes in your infrastructure, the reference model is “Pass-through Authentication with PowerShell Integration”.

It’s fast to deploy and restricts unauthorised users from accessing corporate data. This option blocks unauthorised access, but doesn’t protect Exchange against Internet based attacks. If your Exchange environment is already accessible from the Internet and accessed by your users, then this model is a security improvement. This is the entry-level Exchange protection mechanism, which offers great control but minimal security.

Medium size customers

If you need an Exchange control with minimal changes to your infrastructure, there are a few options to choose from. The reference option is “Enterprise Certificate Authentication”. It’s moderately complex to implement but provides high security, so you get a high return on your investment.

Client certificate authentication provides greater security than standard user credentials, and mitigates password guessing, password lockouts and man-in-the-middle attacks. The “Basic Authentication with PowerShell” option provides almost the same security level as Enterprise Certificate without the benefits of client certificate authentication.

Both methods terminate the traffic in the perimeter (DMZ) network, which protects Exchange from attacks such a Slowloris and SYN flooding, and reduce the load on Exchange. Most firewalls provide a load balancing options, so these options provide greater scope for increased performance and High Availability. These options fit well into organisations that require Disaster Recovery and Business Continuity Planning (DP/BCP). These options rely heavily on the feature set of your firewall vendors.

How to protect your Exchange environment

Highly secure and scalable solution, suitable for large customers

If your organisation needs highly secure and scalable solution for protecting Exchange ActiveSync, then the reference design is “Client Certificate Authentication with Kerberos”.

This option is only available on a small number of firewall and application deliver platforms, notably F5 Big IP and Microsoft TMG. But if you want a highly scaled out Global Server Load Balancing (GSLB) deployment, Matrix42 recommends to evaluate F5 Big IP solution. However this will change over time, so check with your firewall manufacturer.

Client certificate authentication provides greater security than standard user credentials, and mitigates password guessing, password lockouts and man-in-the-middle attacks.

This method terminates the traffic in the perimeter network, which protects Exchange from a range of attacks, and reduces the load on Exchange. It also provides the most mature Disaster Recovery and Business Continuity Planning (DP/BCP) options.

You can deliver a single DC solution or a globally orchestrated GSLB setup across multiple regions, delivering the greatest level of scale, not only technological, but operational scale.

No passwords are used in this design, so account lockouts are not possible. This greatly reduces that number of support calls and increases the overall productivity, ultimately reducing the overall support FTE requirements and cost. In some cases the total cost of ownership savings can ultimately pay for the additional infrastructure costs. If you add the additional productivity saving gained by not locking out users, it’s a considerable saving.

There is a significant level of complexity delivering client certificate authentication with Kerberos Constrained Delegation but it does deliver the greatest level of Confidentiality, Integrity and Availability.

Next Steps

If you are unsure which option to choose, you can directly contact your Matrix42 representative or a Matrix42 Partner (https://www.matrix42.com/en/partners). We are looking forward to help you to designing and implementing your secure mobile management solution with experienced Professional Services employees.

MATRIX42
SMARTER WORKSPACE – BETTER LIFE

How to protect your Exchange environment

Matrix42 AG
Elbinger Str. 7
60487 Frankfurt
Germany
Tel.: +49 (0)6102 - 816-0
Fax: +49 (0)6102 - 816-100
E-Mail: info@matrix42.com
Web: http://www.matrix42.com

MEMBER OF asseco GROUP

Author: Matrix42 Cloud & Mobile Management