Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

HÉLIO MÁRCIO GOMES

SEGURANÇA EM CORREIO ELETRÔNICO BASEADO EM SISTEMAS MICROSOFT

Brasília
2012

HÉLIO MÁRCIO GOMES

SEGURANÇA EM CORREIO ELETRÔNICO BASEADO EM SISTEMAS MICROSOFT

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Me. Marco Antonio Araujo.

Brasília
2013

HÉLIO MÁRCIO GOMES

SEGURANÇA EM CORREIO ELETRÔNICO BASEADO EM SISTEMAS MICROSOFT

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Me. Marco Antônio Araujo.

Brasília, 05 de dezembro de 2013.

Banca Examinadora

_____

Prof. Dr. José Eduardo M. S. Brandão

_____

Prof. Dr. Gilson Ciarallo

Dedicado à memória do saudoso Francisco Lima de Oliveira (Tio Núncio), exemplo de responsabilidade, determinação, superação, ótimo tio, pai e esposo.

AGRADECIMENTOS

Primeiramente a Deus, pela vida.

Aos meus pais, José Gomes dos Anjos e Terezinha Maria das Graças Gomes que me deram amor, carinho e me orientaram a buscar os melhores caminhos e trilhá-los com ética buscando nem sempre o que é melhor para mim, mas sim o bem comum.

A minha esposa Maria José Andrade Gomes, que sempre esteve ao meu lado com palavras de incentivo e amor.

Ao meu orientador, Professor Me. Marco Antônio Araujo, pelas suas importantes contribuições, dedicação e ajuda.

Ao corpo docente do Uniceub, pelo aprendizado.

A todos os meus amigos e colegas do Uniceub, que me ajudaram, incentivaram e partilharam continuamente desta conquista.

Aos amigos de trabalho que sempre me apoiaram e que diretamente ou indiretamente participaram da realização desse sonho.

Só sei que nada sei, e o fato de saber isso, me coloca em vantagem sobre aqueles que acham que sabem alguma coisa.
(Citado por Platão em Apologia de Sócrates)

RESUMO

O Correio eletrônico (e-mail) é uma ferramenta muito utilizada na atualidade, tem um crescimento considerável ano após ano e em muitos casos as informações trafegadas e armazenadas são de extrema importância. Sendo assim o objetivo deste trabalho é apresentar as vulnerabilidades encontradas em sua concepção original e apresentar mecanismos utilizados para garantir a base da segurança da informação em uma infraestrutura de e-mail, mantendo a confidencialidade, disponibilidade e integridade da informação e se possível garantir também o não repúdio. Para isso a organização deve se preparar e garantir um nível satisfatório de segurança, minimizar a exposição de informações a pessoas não autorizadas e garantir que as informações estejam integras e disponíveis para acesso das pessoas autorizadas. O trabalho apresenta a ferramenta Microsoft Exchange Server 2010, suas funcionalidades e boas práticas de segurança como uma alternativa. É implantada uma infraestrutura de e-mail segura utilizando o MS Exchange Server 2010, evitando o acesso não autorizado, o envio de SPAM e mantendo a disponibilidade dos serviços aos usuários. O objetivo do trabalho é alcançado com uma infraestrutura replicada do Active Directory do Windows 2008R2, servidores Mailbox em alta disponibilidade, servidores Hub Transport / Client Acces redundantes, servidores Edge Transport com balanceamento de carga, técnicas criptográficas e treinamento dos usuários para visando uma cultura de segurança na organização.

Palavras-chaves: e-mail. Exchange 2010. Active Directory. Segurança. SPAM.

ABSTRACT

Electronic mail (e-mail) is a tool widely used today, has a significant growth year after year and in many cases the information stored and trafficked is extremely important. Therefore the aim of this paper is to present the vulnerabilities found in its original design and present mechanisms used to ensure the basis of information security and an e-mail infrastructure, maintaining confidentiality, availability and integrity of information and if possible also ensure non-repudiation. For this the organization must prepare itself and ensure a satisfactory level of safety, minimizing exposure of information to unauthorized persons and to ensure that the information are incorrupt and available for access by authorized personnel. The paper presents the Microsoft Exchange Server 2010 tool, its features and good security practices as an alternative. A secure e-mail infrastructure is implemented using MS Exchange Server 2010, avoiding unauthorized access, sending SPAM and maintaining the availability of services to users. The study aim is achieved with a replicated infrastructure of Active Directory from Windows 2008R2, Mailbox servers for high availability, Hub Transport / Client Acces redundant servers, Edge Transport servers with load balancing, cryptographic techniques and training users toward a culture of safety in the organization.

Key words: e-mail. Exchange 2010. Active Directory. Security. SPAM.

SUMÁRIO

INTRODUÇÃO

O correio eletrônico ou simples e-mail é atualmente um sistema digital de grande alcance para troca de mensagens. Até agora, é uma das aplicações mais importantes e de maior sucesso da Internet. (KUROSE; ROSS, 2006).

Tal como o correio normal, o e-mail é um meio de comunicação assíncrono – as pessoas enviam e recebem mensagens quando for conveniente para elas, sem ter de estar coordenada com o horário das outras pessoas. (KUROSE; ROSS, 2006). Por ser um sistema de grande alcance é muito passível de fraudes, essa acontece quando uma pessoa se faz passar por outros na internet. Isso ocorre quando alguém usa as informações de outros, como usuário e senha para acessar contas bancárias, fazer transações e compras on-line. Podendo acontecer devido alguns programas maliciosos que são instalados na máquina sem a percepção do usuário: os vírus e trojan. Uma das formas de propagação e instalação dos vírus ou programas maliciosos muitas vezes se dá por fraudadores que enviam um e-mail falso com assuntos polêmicos que aguça a curiosidade do usuário fazendo-o clicar nos links.

Por essas vulnerabilidades, levando em conta a grande utilização do correio eletrônico no ambiente empresarial, as necessidades crescentes de segurança que afetam a confidencialidade, disponibilidade e integridade das informações, esse trabalho acadêmico propõe o estudo para adicionar mecanismos de segurança em uma infraestrutura de correio eletrônico, Microsoft Exchange 2010, de forma que garanta a transferência segura de e-mail interno e externo e que possa assegurar a base da segurança da informação em dados armazenados nos servidores e em trânsito entre os servidores de transporte. Os mecanismos de segurança do MS Exchange Server 2010 visam minimizar o campo de ação dos fraudadores, seja na implantação de softwares maliciosos nas estações de trabalho, ou na captura de informações em trânsito que possa servir de base para uma futura fraude. Sendo assim serão utilizados mecanismos criptográficos, filtros AntiSpam, filtros antivírus e mecanismos que atestem que quem encaminha a mensagem é a pessoa que se diz ser.

Este trabalho tem como objetivo principal apresentar as funcionalidades necessárias para implementar uma infraestrutura de e-mail seguro com a ferramenta Microsoft Exchange Server 2010, seguindo as boas práticas e visando alcançar a base da segurança da informação: confidencialidade, integridade e disponibilidade. Tendo como finalidade a apresentações de padrões de segurança de e-mail e alguns mecanismos que podem ser implantados nas organizações visando diminuir o campo de ataques e como esses mecanismos podem ser alcançados utilizando as tecnologias encontradas no Microsoft Exchange Server 2010 de modo que possa minimizar as fraudes que se iniciam com as vulnerabilidades no e-mail. Como objetivos específicos:

- Descrever o funcionamento de uma infraestrutura de e-mail;
- Apresentar as principais vulnerabilidades do e-mail convencional e as principais técnicas que visam explorar essas vulnerabilidades;
- Descrever a infraestrutura necessária para implementar o Exchange Server 2010;
- Abordar as ferramentas de segurança da informação e como implementar uma infraestrutura de e-mail segura utilizando o Exchange Server 2010 e assim alcançar as boas práticas da segurança da informação.

O serviço de correio eletrônico é um dos serviços de comunicação mais usado na Internet. Este serviço em geral provê pouca segurança e privacidade, permite facilmente vários tipos de fraudes e uso indevidos. No meio corporativo o Exchange Server, (em suas mais variadas edições), é muito utilizado como ferramenta de e-mail. Mas a grande maioria das organizações não se preocupam em implantar os mecanismos de segurança que a ferramenta oferece, deixando assim, as vulnerabilidades do serviço de e-mail convencional.

Diante dessa realidade, as implementações que não seguem as boas práticas da segurança da informação permitem a exposição de informações confidenciais a pessoas não autorizadas, ou seja, não garante que a troca de mensagem seja segura, confiável e disponível. Configurações fora das melhores práticas também podem contribuir para a proliferação de SPAM, ou seja, podem ser

explorados servidores de transporte de uma organização para encaminhar e-mails indevidos.

Sendo assim, para garantir o nível satisfatório de segurança, os servidores devem estar bem configurados, possibilitando a menor exposição a fraudes, uso indevido da informação, ataques bem sucedidos e a proliferação de SPAM. Para alcançar esses objetivos será implementado servidores Exchange Server 2010 de forma segura simulando um ambiente corporativo, visando dificultar a ação de hackers, ou de vermes que tentam aproveitar furos de segurança no serviço de e-mail e ao mesmo tempo abordado tecnologias que de alta disponibilidade garantindo assim os pilares da segurança da informação: confidencialidade, integridade e disponibilidade.

Para discorrer a respeito, o presente trabalho foi estruturado em 3 capítulos.

No primeiro capítulo, apresenta-se a estrutura do correio eletrônico como foi concebido com seus principais protocolos e forma de funcionamento. Apresenta ainda o sistema de correio eletrônico da Microsoft; o Exchange Server 2010, a infraestrutura que o suporta e os papeis que podem ser desempenhado por cada servidor em uma organização de mensageria.

No segundo capítulo é apresentada uma visão geral de segurança no Exchange Server 2010.

No terceiro capítulo se apresenta uma concretização dos dados abordados nos capítulos anteriores, onde se apresenta a implantação de uma organização do Exchange Server 2010 com os passos e configurações mínimas de forma que se consiga a disponibilidade, confidencialidade e integridade das mensagens armazenadas, ou em trânsito nos servidores de transporte, ou acessada nos clientes de correio eletrônico.

1 SISTEMA DE CORREIO ELETRÔNICO

1.1 Infraestrutura

Os primeiros sistemas de correio eletrônico consistiam simplesmente em protocolos de transferência de arquivos. À medida que as pessoas ganharam experiência, se propôs sistemas de correio eletrônico mais elaborados. As propostas mais relativas foram publicadas nas RFC 821 (protocolo de transmissão) e RFC 822 (formato da mensagem). Revisões menores, publicadas nas RFCs 2821 e 2822, se tornaram padrões da Internet, mas todos ainda se referem ao correio eletrônico da Internet como RFC 822. (TANENBAUM, 2003).

Em geral o correio eletrônico consiste em dois subsistemas: os agentes do usuário, que permite a leitura e envio de mensagens e os agentes de transferência de mensagem, responsável por deslocar as mensagens da origem ao destino. Os agentes dos usuários são programas locais para interagir com o sistema de correio eletrônico. Normalmente os agentes de transporte são daemons do sistema, ou seja, processos executados no segundo plano que movem as mensagens de correio eletrônico pelo sistema. (TANENBAUM, 2003).

No geral os sistemas de correio eletrônico admitem cinco funções básicas:

- Composição: processo de criação e resposta de mensagens. Qualquer editor de texto pode ser usado para compor o corpo da mensagem, mas o sistema em si pode auxiliar com o endereçamento e com os inúmeros campos de cabeçalho associados a cada mensagem.
- Transferência: deslocamento da mensagem entre o remetente e o destinatário, em geral estabelece uma conexão com o destino, ou com alguma máquina intermediária, a transmissão da mensagem e o encerramento da conexão.
- Geração de relatório: permite obter informações do que ocorreu com a mensagem, informado se foi entregue, rejeitada, perdida.

- Exibição: as mensagens recebidas necessitam ser trabalhadas para que as pessoas possam ler visualizar imagens, executar arquivos de vídeo.
- Disposição: é a ultima etapa e refere-se ao que o destinatário faz com a mensagem depois de recebê-la.

Além dos serviços básicos, alguns sistemas de correio eletrônico, principalmente os sistemas voltados para empresas, oferecem uma grande variedade de recursos avançados.

Hoje o correio eletrônico é amplamente utilizado para comunicação em uma empresa, ou entre empresas. Permitindo que funcionários fisicamente distantes cooperem em projetos mesmo separados por muitos fusos horários.

Uma ideia fundamental em todo sistema de correio eletrônico é a distinção entre o envelope e o conteúdo. A mensagem é encapsulada pelo envelope, esse contem todas as informações que são utilizadas no transporte, como endereço de destino, prioridade, nível de segurança, sendo todas distintas da mensagem em si. Os agentes de transporte de mensagem utilizam o envelope para executar o roteamento.

A mensagem dentro do envelope consiste em duas partes: o cabeçalho e o corpo. O cabeçalho contém informações de controle para o agente do usuário. O corpo da mensagem diz respeito apenas ao destinatário. (TANENBAUM, 2003).

1.1.1 Principais Protocolos

Para o envio e busca de mensagens podem ser utilizados os seguintes protocolos:

1.1.1.1 POP3 (Post Office Protocol)

É um protocolo para pegar e-mails em servidores remotos. Os clientes podem fazer logon em um servidor Exchange e então usar o POP3 para fazer o download de suas mensagens de e-mail para usá-las off-line. (STANEK, 2004)

Utiliza qualquer endereço IP disponível no servidor e responde nas portas 110 e 995. A porta 110 é usada para comunicação padrão, ao passo que a porta 995 é usada para comunicação SSL. (STANEK, 2004)

Figura 01: Principais Comandos do POP3.

Principais comandos do POP3	
USER *nome*	Identificador do cliente
PASS *senha*	Senha para acesso
DELE *msg*	Elimina a mensagem identificada pelo némero *msg*
LIST [*msg*]	Lista assunto do e-mail de número *msg*
RETR *msg*	Busca no servidor o conteúdo do e-mail de número *msg*
RSET	Retira marcas de eliminação de e-mail
STAT	Indica o número de e-mail destinados ao usuário e o espaço usado
QUIT	Muda para atualização e o servidor elimina todos os e-mails marcados

Fonte: elaborada pelo autor do trabalho.

1.1.1.2 IMAP (Internet Message Access Protocol)

Protocolo para leitura de e-mail. A versão 4 é usada para fazer download dos cabeçalhos de mensagens, podendo em seguida lê-las individualmente, enquanto estão on-line. (STANEK, 2004)

Usa normalmente a porta 143 no modo TLS/SSL na porta 993 (Transport Layer Security / Secure Sockets Layer). O usuário pode manipular suas mensagens e pastas a partir de computadores diferentes em diversas localidades sem que seja necessária a transferência das mensagens do servidor para o computados. As mensagens podem ser acessadas de um computador portátil durante uma viagem, no micro de casa ou do trabalho. O protocolo IMAP também permite o acesso das mensagens armazenadas localmente, desde que o usuário tenha feito o sincronismo das mensagens armazenadas no servidor com o seu disco local. (STANEK, 2004)

1.1.2 Funcionamento

Segundo Cavalcante, Filho e Brasileiro, (2004). O SMTP (Simple Mail Transfer Protocol) é o padrão TCP/IP que especifica como o serviço de correio eletrônico transmite mensagem na Internet. A estrutura de uma máquina que implementa o SMTP inclui as caixas postais dos usuários, uma ou mais área para enfileiramento de mensagens em trânsito e um ou mais processos rodando em background (daemons) para entrega e recebimento dos e-mail. Abaixo descrição de cada componente:

- Caixa postal – É uma área de armazenamento, na qual as mensagens permanecem até que o usuário as elimine ou as transfira para outra área. É a versão eletrônica da caixa postal do sistema de correio tradicional.
- Áreas de enfileiramento das mensagens – É uma área onde as mensagens são armazenadas para futura transmissão.
- Agente usuário – O UA é o software de correio eletrônico que permite o usuário confeccionar, enviar, receber e ler mensagens, bem como manipular a caixa postal.

Agente de transferência de mensagens – O MTA é o programa que coloca a mensagem diretamente na caixa postal, quando o UA de destino está ligado a ele, ou encaminha para ele, ou encaminha para a máquina de destino, usando o SMTP. Durante o diálogo entre duas máquinas que implementam o SMTP, a máquina de origem age como cliente SMTP, e a máquina de destino age como servidor SMTP aceitando as mensagens e as colocando na caixa postal do destinatário. As máquinas que rodam MTAs são conhecidas como servidores de e-mail.

Esse funcionamento é transparente para os usuários, pois as mensagens são escritas no cliente de e-mail (UA), os dados são formados em padrão da RFC 2822 em seguida enviado ao MTA que usa o protocolo SMTP para fazer a comunicação com o próximo servidor. Para prosseguir a transmissão faz-se uma consulta na entrada Mail eXchanger (MX) no Domain Name Service (DNS) do domínio, e depois de verificar o endereço Internet Protocol (IP) do servidor de destino estabelece a comunicação com o servidor e faz a entrega da mensagem. Um domínio pode ter várias entradas MX que servem para balanceamento de carga ou apenas como redundância.

1.2 Formatos da Mensagem de E-mail

A seguir é mostrado o código fonte que forma uma mensagem. As linhas 1 a 13 formam o cabeçalho, onde ficam alguns campos From, To, Subject que são visíveis em um MUA. A linha 14, que é uma linha em branco, separa o cabeçalho do corpo da mensagem. As linhas 15 a 18 fazem parte do corpo de uma mensagem.

Figura 02: Código Fonte de Uma Mensagem.

```
1 From – Thu Dec 13 18:12:25 2007
2 X-DeliveredTo: edson@three.p2pmail.com
3 X-RecievedDate: Thu Dec 13 18:12:18 BRST 2007
4 Received: by EricDaugherty JES SMTP two.p2pmail.com from client: 127.0.0.1
5 Message-ID: <45637377.8010909@two.p2pmail.com>
6 Date: Thu, 13 Dec 2007 18:12:18 -0200
7 From: esdon < edson@three.p2pmail.com>
8 User-Agent: Thunderbird 2.0.0.6 (X11/20071022)
9 MIME-Version: 1.0
10 To: edson@three.p2pmail.com
11 Subject: Ola
12 Content-Type: text/plain; charset=ISO-8859-1; format=flowed
13 Content-Transfer-Encoding: 7bit
14
15 Ola,
16 Tchau
17
18 User2
```

Fonte: elaborada pelo autor do trabalho.

1.2 Mime

A RFC 822 define um formato para mensagens de texto que são enviados por meio de e-mail. Ele tem sido o padrão de mensagem de correio baseado na internet e continua sendo muito usado. No contexto da RFC 822, as mensagens são vistas como tendo um envelope e conteúdo. O envelope contém qualquer informação que seja necessária para conseguir transmissão e entrega. O conteúdo compõe o objeto a ser entregue ao destinatário. O padrão RFC 822 só se aplica ao conteúdo. Porém, o padrão do conteúdo inclui um conjunto de campos de cabeçalho que pode ser usado pelo sistema de correio para criar o envelope, e o padrão visa a facilitar a aquisição dessa informação pelos programas. (STALLINGS, 2007)

O protocolo de envio de e-mail como concebido previa o envio de e-mails em formato de mensagens de texto, essa abordagem é insuficiente para as necessidades dos usuários de correio cuja linguagem requer o uso de conjuntos de caracteres mais ricos do que ASCII. Outra limitação é o de limitar o conteúdo de mensagens de correio eletrônico para linhas relativamente curtas, por exemplo, 1000 caracteres ou menos de 7bit ASCII. Mime é um protocolo que foi definido com o objetivo de permitir a inclusão de dados não ASCII via e-mail. Isso porque o protocolo SMTP – usado para transferência de e-mail – trabalha apenas com caracteres NTVASCII.

O padrão MIME foi proposto para suprir a necessidade de enviar arquivos anexados junto a mensagem de e-mail. São definidos pelas RFC 2045, RFC 2046, RFC 2047, RFC 2048 e RFC 2049. O padrão MIME codifica os arquivos anexados a uma mensagem, formatando-as em modo texto e inserindo-os na mensagem. Com essa abordagem não foram necessárias alterações no protocolo SMTP.

Foram definidas novas variáveis de cabeçalhos, que podem ser inclusas no cabeçalho de mensagens. Estes campos possuem informações sobre o corpo da mensagem, conforme descrito:

- MIME-Version: informa que a mensagem tem o formato MIME;
- Content-ID: identifica o conteúdo do corpo da mensagem;
- Content-Type: especifica o tipo de arquivo ou subtipo de dados incluídos na mensagem;
- Content-Transfer-Encoding: define vários métodos para a representação de dados binários em formato texto ASCII;
- Content-Description: descreve o conteúdo do corpo da mensagem, decifrando quando o objeto não pode ser lido, como por exemplo, arquivo de música.

Também são definidas as codificações de conteúdo de transferência (Content-Transfer-Encoding) onde são apresentados vários métodos para conversão de um dados binário em ASCII. Podem ser:

- 7bit: indica que o texto é codificado em 7bits (conjunto de caracteres US-ASCII);

- 8bit: mostra que a mensagem contém texto com alguns caracteres que necessitam de 8bits para serem codificados (conjunto de caracteres não US-ASCII). Caso uma mensagem deste tipo passe por uma zona da rede que permite transportar somente caracteres de 7bits, todos os caracteres que necessitam de 8bits chegarão ao destino com erros;

- Binary: refere-se a dados em que qualquer sequencia de octetos é permitida;

- Quated-printable: codifica textos simples com caracteres US-ASCII, transformando, por exemplo, a palavra Avião para Avi=E3o;

- Base64: demonstra a existência de binários codificados. Todos os caracteres são codificados como grupo de caracteres de 7 bits, de tal modo que o binário não será alterado ao trafegar pela rede.

Através do padrão MIME, um usuário pode incluir arquivos em um e-mail de diferentes formatos com diferentes codificações. Grande parte do sucesso do padrão MIME deve-se ao fato do mesmo ser transparente aos servidores de e-mail, pois o corpo de cada e-mail é visualizado em formato ASCII, conforme a definição da RFC 2822. Todo o processamento de codificação e decodificação das mensagens de e-mail é realizado pelos programas clientes (MUA), durante o envio e a recepção.

O MIME é um protocolo complementar ao SMTP, não sendo responsável pela transmissão dos dados. Além disso, seu uso não está restrito ao SMTP, podendo ser utilizado com qualquer protocolo de envio de e-mail. Ele resolve as deficiências de limitações no conteúdo das mensagens, mas não insere segurança, pois o conteúdo pode ser interceptado e lido por pessoas indevidas, essa deficiência é resolvida com a utilização de técnicas criptográficas que serão abordadas.

1.3 Vulnerabilidades em Correio Eletrônico

O SMTP, definido no RFC 5321, está no coração do correio eletrônico da Internet. (KUROSE; ROSS, 2010). É usado para transferir mensagens de servidores de correio remetentes para servidores de correio destinatário, não se preocupando com alguns aspectos de segurança, já que no inicio a Internet era restrito a comunidades acadêmicas e utilizado para fins científicos. Hoje é uma ferramenta muito utilizada no dia a dia das pessoas, seja para uso organizacional (empresa), ou pessoal (gmail, hotmail). Essa popularização trouxe uma série de vulnerabilidades, que no início era insignificante, como vírus, falsificação de identidade, SPAM, captura de mensagens em trânsito que comprometem a segurança do e-mail.

O e-mail é uma das formas mais comuns de espalhar vírus de uma organização para outra, ou para e-mail particular. Sendo uma preocupação adicional para segurança em correio eletrônico, pois pode tornar o sistema inutilizável destruindo arquivos de sistema operacional, ou roubar dados dos usuários que podem ser utilizados para transações eletrônicas fraudulentas. Geralmente são encaminhados em arquivos anexados aos e-mails, e se lido ou aberto infecta a estação de trabalho e pode ser propagados para outras máquinas da rede, ou se duplicar para todos os contatos do usuário.

Outra vulnerabilidade está nas mensagens não solicitadas (SPAM) que oneram os servidores afetando seu desempenho, podem servir como porta de entrada de vírus infectando as máquinas e afetar os usuários do serviço de correio de várias formas, o antispam.br enumera algumas:

- Não recebimento de e-mail: por parte das caixas com limite de tamanho de caixa de correio;
- Gasto desnecessário de tempo: para cada spam recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como spam e removê-lo da caixa postal;
- Perda de produtividade: Para quem usa o e-mail como ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à tarefa de

leitura de e-mails, além de existir a chance de mensagens importantes não serem lidas, serem apagadas por engano ou lidas com atraso;

- Conteúdo improprio ou ofensivo: Como a maior parte dos spams é enviada para conjuntos aleatórios de endereços de e-mail, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo;

- Prejuízos financeiros causados por fraudes: O spam tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos, projetados para furtar dados pessoais e financeiros. Esse tipo de spam é conhecido como phishing/scam. O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas nesse tipo de mensagem fraudulenta.

O Simple Mail Transfer Protocol (SMTP) não trata a possibilidade de interceptação de mensagens, ou falsificação de remetente (causado pela característica de funcionamento que para se ler o e-mail é necessário se acessar a caixa com uso de usuário e senha, mas para encaminhar o e-mail não existe essa necessidade, o que permite que um usuário forje a identificação do remetente).

Como no inicio do e-mail não foi previsto essas vulnerabilidades, cabe ao projetista da solução de correio eletrônico elaborar uma forma eficiente para diminuir ao máximo a incidência vírus, spam, interceptação de mensagens ou falsificação de remetente.

1.4 Visão Geral do Microsoft Exchange 2010

O Microsoft Exchange Server 2010 é a plataforma de sistema de mensagem da Microsoft e apresenta um conjunto novo e sofisticado de tecnologias, recursos e serviços para a linha de produtos do Exchange Server. Novos recursos e funcionalidades no Exchange server 2010 dão suporte a vários conceitos importantes:

- Flexibilidade e confiabilidade: A pressão para otimizar a infraestrutura de TI e atender às mudanças nas condições comerciais demanda agilidade e isso significa investimentos em soluções que forneçam uma opção segura para a organização. O Exchange 2010 dá a flexibilidade para personalizar a implantação com base nas necessidades únicas da organização e uma forma simplificada de ajudar a manter a disponibilidade contínua do e-mail para os usuários.

- Acesso em qualquer lugar: Os aperfeiçoamentos no Exchange 2010 ajudam os usuários a fazerem mais, ao auxiliá-los a acessarem toda a comunicação de e-mail em praticamente qualquer plataforma.

- Proteção e conformidade: O Exchange 2010 entrega uma nova funcionalidade de retenção e arquivamento de e-mail integrada, possibilitando a pesquisa granular em várias caixas de correio e a guarda de documentos imediato. Ele também ajuda a proteger a comunicação de correio eletrônico da empresa por meio dos recursos de controle das informações que são gerenciadas de modo centralizado. Isso inclui a possibilidade de interceptar, moderar, criptografar e bloquear mensagem de e-mail com mais eficiência. Juntas, essas funcionalidades fornecem um conjunto flexível de opções de proteção e controle, independente de se desejar aplicar automaticamente os controles ou a capacidade de possibilitar aos usuários que eles implementem a proteção dos dados.

1.4.1 Infraestrutura de Suporte ao Microsoft Exchange 2010

O Exchange Server 2010 faz uso intenso do Active Directory. Cada atribuição (role) do Exchange Server 2010 deve acessar o Active Directory para recuperar informações sobre destinatários e outras atribuições de servidores Exchange. (STANEK, 2011).

Para compreender como o Microsoft Exchange Server 2010 funciona e como pode ser aplicado segurança no mesmo é necessário conhecer um pouco da infraestrutura do Active Directory que dá suporte a implantação de uma organização do Exchange Server 2010. O Active Directory Domain Services e seus serviços relacionados formam a base das redes corporativas em execução no Microsoft

Windows uma vez que, em conjunto, eles funcionam como ferramentas para armazenar informações sobre identidades dos usuários, computadores e serviços. E assim fornecer um mecanismo com o qual usuários e computadores possam acessar recursos na empresa. (HOLME; RUEST; KELLINGTON, 2011).

1.4.1.1 Active Directory

Como mencionado anteriormente o Active Directory fornece uma solução IDA (Identidade e acesso) para redes corporativas em execução no Windows. O IDA é necessário para manter a segurança de recursos corporativos como arquivos, e-mails, aplicativos e banco de dados. Uma Infraestrutura IDA deve ter as seguintes funcionalidades:

- Armazenar informações sobre usuários, grupos, computadores e outras identidades;

- Autenticar uma identidade: Não será concedido acesso ao usuário a menos que seja verificado e constatado que a identidade apresentada na solicitação é válida. Para validar a identidade o usuário apresenta segredos conhecidos apenas pelo o usuário e a infraestrutura IDA. Os segredos são comparados às informações no armazenamento de identidades, processo chamado de autenticação. (HOLME; RUEST; KELLINGTON, 2011).

- Controle de acesso: A infraestrutura IDA é responsável por proteger as informações confidenciais. O acesso a informações confidenciais deve ser gerenciado de acordo com as diretivas da empresa. A ACL no documento reflete a diretiva de segurança composta das permissões que estão especificadas o nível de acesso a determinada identidade. (HOLME; RUEST; KELLINGTON, 2011).

- Trilha de auditoria: Permite controlar as modificações e atividades dentro da infraestrutura IDA, fornecendo mecanismos por meio do qual é possível gerenciar e auditar. (HOLME; RUEST; KELLINGTON, 2011).

- Active Directory Domain Services (AD DS): Projetado para fornecer um repositório central ao gerenciamento de identidades dentro de uma

organização. AD DS fornece serviços de autenticação e autorização em uma rede e suporta o gerenciamento de informações e serviços compartilhamento, permitindo aos usuários localizar qualquer componente. O AD DS é a principal tecnologia do Active Directory e deve ser implantado em cada rede que executa sistemas operacionais Windows. (HOLME; RUEST; KELLINGTON, 2011).

- Active Directory Lightweigth Directory Services (AD LDS): O AD LDS é um subconjunto do AD DS, ambos estão baseados no mesmo código básico. O AD LDS só armazena e replica informações relacionadas a aplicativos. É comumente utilizado por aplicativos que exigem um armazenamento de diretório, mas não exige que as informações sejam replicadas de uma maneira tão ampla como, por exemplo, os controladores de domínio. (HOLME; RUEST; KELLINGTON, 2011).

- Active Directory Certificate Services (AD CS): Utilizado para configurar uma autoridade certificadora para emitir certificados digitais como parte de uma infraestrutura de chave pública que vincula a identidade de uma pessoa, dispositivo ou serviço a uma chave privada correspondente. (HOLME; RUEST; KELLINGTON, 2011).

- Active Directory Rights Management Services (AD RMS): É uma tecnologia de proteção das informações que permite implementar modelos persistentes de diretiva de uso que definem o uso autorizado e não autorizado, seja on-line, off-line, dentro ou fora do firewall. (HOLME; RUEST; KELLINGTON, 2011).

- Active Directory Federetion Services (AD FS): Permite que uma organização estenda a solução IDA para multiplataforma, incluindo ambientes Windows e não Windows, e projetar identidades e acesso cruzando limites de segurança para parceiros confiáveis. Os usuários são autenticados em uma rede, mas podem acessar recursos em outra. O AD FS suporta parcerias porque ele permite que diferentes organizações compartilhem o acesso a aplicativos de extranet baseando-se em suas próprias estruturas AD DS

interna para fornecer o processo de autenticação real. (HOLME; RUEST; KELLINGTON, 2011).

1.4.1.2 Além da Solução IDA

O Active Directory oferece mais do que uma simples solução IDA. Ele também fornece os mecanismos para suportar, gerenciar e configurar recursos nos ambientes de rede distribuída. Um conjunto de regras, o esquema, define classes de objetos e atributos que podem estar contidos no diretório. [Holme, Ruest, Kellington, 2011]. Sendo assim é importante uma abordagem básica nos componentes de uma infraestrutura do Active Directory.

- Armazenamento de dados do Active Directory: O AD DS armazena as identidades em um diretório, armazenamento de dados hospedados nos controladores de domínio, o diretório é um arquivo chamado Ntds.dit e fica localizado em controladores de domínio. O banco de dados é dividido em várias partições, incluindo o esquema, configuração, catálogo global e o contexto de nomeação de domínios que contém os dados sobre objetos dentro de um domínio.

- Controladores de domínio (DC): São servidores que executam a função de AD DS. Como parte dessa função, eles também executam o serviço de Kerberos Key Distribution Center (KDC), que realiza a autenticação e outros serviços do Active Directory. (HOLME; RUEST; KELLINGTON, 2011).

- Domínios: É uma unidade administrativa dentro da qual certas capacidades e características são compartilhadas. Além disso, um domínio é um escopo das diretivas administrativas, com as diretivas de complexidade de senha e bloqueio de conta. Essas diretivas configuradas em um domínio afetam todas as contas no domínio e não afetam contas em outro domínios. (HOLME; RUEST; KELLINGTON, 2011).

- Floresta: É uma coleção de um ou mais domínios do Active Directory. O primeiro domínio instalado em uma floresta é chamado domínio raiz da floresta. Uma floresta contém uma única definição de configuração de rede e

uma única instancia do esquema de diretório. Ou seja uma floresta define um limite de segurança. (HOLME; RUEST; KELLINGTON, 2011).

- Árvore: O Namespace DNS dos domínios em uma floresta cria árvores dentro da floresta. Se um domínio for subdomínio de outro domínio, os dois domínios serão considerados uma árvore. (HOLME; RUEST; KELLINGTON, 2011).

- Sites: É um objeto que representa uma parte da empresa dentro da qual a conectividade de rede é boa. Um site define um limite de uso de replicação e serviços. (HOLME; RUEST; KELLINGTON, 2011).

1.4.2 Implantação do Microsoft Exchange Server 2010

Cada implementação do Exchange tem três camadas em sua arquitetura. A primeira é a network layer (camada de rede), ela fornece os elementos básicos para as comunicações entre computadores e recursos essenciais de resolução de nomes. A camada de rede tem componentes físicos e lógicos. Os componentes físicos incluem os endereços IP, link para rede local (LAN) ou rede remota (WAN) usada pelos sistemas de mensagens, assim como os roteadores que conectam esses links, e firewalls que protegem a infraestrutura. Os componentes lógicos são as zonas de DNS (Domain Name System) que definem os limites de nomes e contêm os registros de recursos essenciais necessários para a resolução de nomes.

A segunda camada compreende o Directory Layer (camada de diretório), essa fornece os elementos básicos necessários para a autenticação, autorização e replicação.

A terceira camada é a messaging layer (camada de transmissão de mensagem), fornece os elementos básicos para transmissão de mensagens e colaboração. Essa camada tem componentes físicos e lógicos. Os físicos incluem os servidores Exchange, que determinam como as mensagens são entregues, e os conectores de mensagem, que determinam como as mensagens são roteadas para fora dos limites de roteamento do servidor Exchange. Os componentes lógicos especificam os limites organizacionais para a transmissão de mensagens, caixas de correio usadas para armazenar as mensagens, pastas públicas usadas para

armazenar dados e listas de distribuição usadas para distribuir as mensagens para múltiplos destinatários. (STANEK, 2011).

1.4.3 Atribuições de Transmissão de Mensagens

Como visto anteriormente o Exchange 2010 têm três camadas na sua arquitetura. A camada de transmissão de mensagem é onde se encontra as atribuições (rules) do Exchange Server. Os servidores Exchange no núcleo da camada de transmissão de mensagem podem operar nas atribuições a seguir:

- Mailbox Server: Servidor back-end que hospeda as caixas de correio, pastas públicas e dados relacionados às mensagens, como listas de endereços, agendamento de recursos e itens de reunião. Para obter uma alta disponibilidade dos bancos de dados de caixa de correio pode ser usado os grupos de disponibilidade de banco de dados (database availability groups). (STANEK, 2011).

- Client Access Server: Servidor de camada intermediária que aceita as conexões para o Exchange Server realizadas a partir de vários clientes. Esse servidor hospeda os protocolos usados por todos os clientes durante a verificação de mensagens. Em rede local os cliente do Outlook MAPI são conectados diretamente ao servidor Client Access para verificar os e-mails. Os usuários remotos podem verificar seus e-mails pela Internet usando o Outlook Anywhere, Outlook Web App, Exchange ActiveSync, POP3 ou IMAP4. (STANEK, 2011).

- Unified Messaging Server: Servidor de camada intermediária que integra um sistema PBX com o Exchange Server 2010, permitindo que mensagem de voz e fax seja armazenada em uma caixa de correio do usuário. (STANEK, 2011).

- Hub Transport Server: Servidor de roteamento de mensagens que manipula o fluxo, o roteamento e a entrega de mensagens na organização do Exchange. Esse servidor processa todas as mensagens que são enviadas dentro da organização entes de serem enviadas para uma caixa de correio ou roteadas para usuários externos. Para atender requisitos de conformidade

regulatório ou organizacional, o Hub Transport pode registra, ou lançar no diário (jornal), as mensagens e adicionar ressalva. (STANEK, 2011).

- Edge Transport Server: Servidor de roteamento adicional que roteia as mensagens para dentro e para fora da organização do Exchange. Esse servidor é projetado para ser implantado em uma rede de perímetro (perimeter network –DMZ) da organização e é usado para estabelecer um limite seguro entre a organização e a Internet. Processa as mensagens para se proteger contra alguns tipos de mensagens de spam e vírus, e roteia todas as mensagens aceitas para um servidor Hub Transport dentro da organização. (STANEK, 2011).

2 VISÃO GERAL DE SEGURANÇA NO EXCHANGE SERVER 2010

Segundo a norma ABNT NBR ISO/IEC 17799:2005 segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio e minimizar o risco do negócio. É obtida a partir de um conjunto de controles adequados que incluem política, processos, procedimentos, estrutura organizacionais, funções de software e hardware.

Uma infraestrutura de correio eletrônico baseado no Exchange Server 2010 tem a capacidade de atender os pilares da segurança da informação podendo alcançar confidencialidade, integridade, disponibilidade e o não repudio. Ele foi projetado para dar mais proteção e segurança a uma infraestrutura de correio eletrônico. O conceito se inicia na instalação, onde se tem uma implantação baseada em funções de servidor e que instala apenas os códigos necessários para a função de servidor selecionada, minimizando a superfície de ataque. A instalação permite apenas os serviços necessários para a função de servidor específica, e cria exceções de firewall necessárias no firewall do Windows com segurança avançada permitindo a comunicação apenas com esses serviços. Visando garantir os pilares da segurança da informação é abordado abaixo as técnicas e modelos disponíveis no Microsoft Exchange 2010 que podem aumentar a segurança na infraestrutura de correio eletrônico.

2.1 Modelos de Permissões

O padrão de permissões no Exchange 2010 é baseado em dois modelos. O primeiro é o modelo padrão do Active Directory, que usa permissões de usuários, contatos e grupos de segurança que tem direitos atribuídos a eles. A segunda foi introduzida no Exchange 2010, que é um novo modelo denominada RBAC (role-basead access control), esse modelo é implementado em conjunto com o modelo de permissão padrão. (STANEK, 2011).

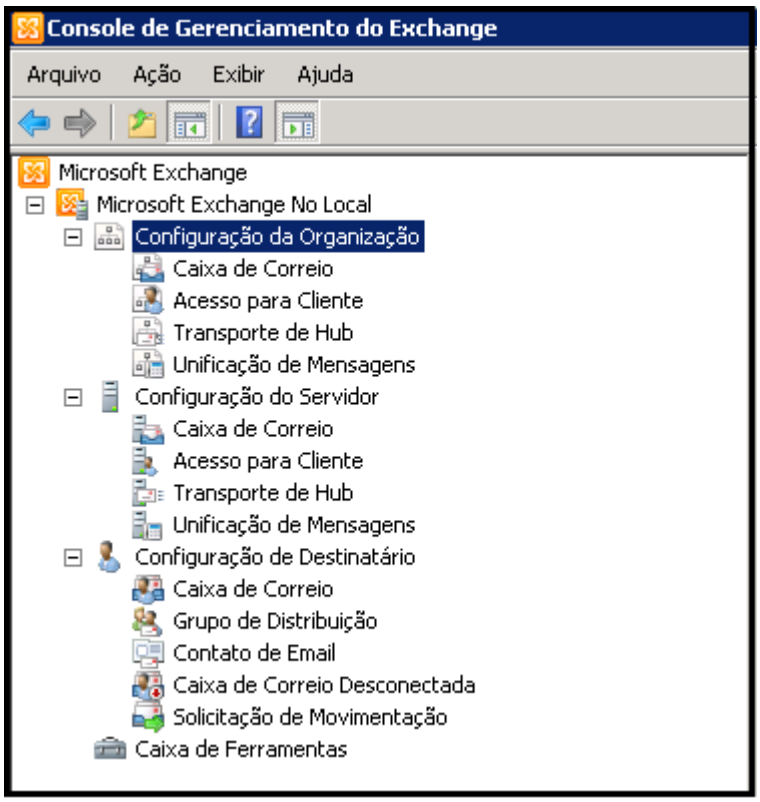
2.1.1 Permissão Padrão

A maioria das informações do Exchange é armazenada no Active Directory. Usuários, contatos e grupos são representados no Active Directory como objetos. Esses objetos têm muitos atributos que determinam como são usados. As permissões atribuídas aos objetos são os atributos mais importantes, elas concedem

ou negam acesso aos objetos e recursos. As permissões atribuídas a um objeto podem ser aplicadas diretamente, ou serem herdadas. (STANEK, 2011).

No Exchange Server 2010, as permissões são herdadas através da hierarquia organizacional. A raiz da hierarquia é o nó Organização. Todos os outros nós da árvore herdam as permissões desse nó.

Figura 03:Representação do Console de Gerenciamento do Exchange - Nó Configuração da Organização.



Fonte: “elaborada pelo autor do trabalho”.

2.1.2 Permissão Baseada em Atribuições

Como verificado anteriormente no Exchange Server 2010 uma nova metodologia é usada para gerenciar permissões de acesso do usuário e funcionalidades administrativas. O RBAC provê mais eficiência e controle granular do que observado nas permissões padrões do Exchange que era única forma de atribuir permissões nas versões anteriores do Exchange Server.

O controle de acesso baseado em atribuições usa a definição de uma atribuição para designar as tarefas de gerenciamento que um usuário, ou grupo de usuários podem executar. Por padrão é atribuído varias atribuição de gerenciamento

nativo. Cada atribuição nativa atua como um agrupamento lógico de permissões que especifica as ações de gerenciamento que os submetidos à atribuição podem executar. O Exchange permite ainda que aos administradores criarem suas atribuições personalizadas. (STANEK, 2011). Esse tipo de controle de acesso visa o principio do menor privilégio, onde se concede apenas os privilégios necessários para a execução de ações.

Ao trabalhar com permissões baseadas em atribuição devem ser considerados os seguintes casos:

- Pode ser definido permissões para qualquer conta de usuário habilitada para e-mail.
- Para qualquer conta de segurança universal. Definindo uma atribuição a um grupo é concedido aos membros do grupo a capacidade de executar uma ação de gerenciamento específico.
- Não pode ser definido permissões baseada em atribuição a grupos de segurança com escopo de domínio local ou global e a grupos de distribuição independente do escopo.

2.2 Auditoria

2.2.1 Auditoria em Nível de Servidor

A auditoria permite o controle do que está acontecendo, é possível usar a auditoria para coletar informações relacionadas a logons, logoffs, uso de permissões e muito mais. Sempre que ocorrer uma ação que foi definida em uma configuração de auditoria um Log é gerado e fica armazenado em log de segurança do sistema e pode ser acessado para revisão. É recomendada a utilização de um servidor de Logs para armazenar os logs por um período maior, ou ser adquirido uma ferramenta de terceiro para gerenciar e armazenar os logs.

A auditoria pode ser configurada localmente nos servidores que desempenham a função de servidores de e-mail, para isso é necessário acessar a ferramenta Local Security Policy e fazer as definições de auditoria desejado. Ou podem ser configuradas no domínio por meio de um objeto Group Policy do Active

Directory (GPO), para configurá-la é necessário acesso ao Grupo Policy Management Console (GPMC), que depois de instalado pode ser acessado via menu Administrative Tools. As seguintes opções de auditoria são encontradas:

- Audit Account Logon Events: Controla a autenticação de conta de usuário durante o logon. Esses eventos são gerados no computador de autenticação quando o usuário é autenticado.

- Audit Account Management: Controla o gerenciamento de conta por meio do Usuários e Computadores do Active Directory. Os eventos são gerados sempre que um usuário, computador ou conta de grupo são criados, modificados, ou excluídos.

- Audit Directory Services Access: Controla o acesso ao Active Directory, eventos gerados quando usuários ou computadores acessam o diretório.

- Audit Logon Events: Controla os eventos de logon local.

- Audit Object Access: Controla o uso de recursos do sistema para caixas de correio, information store e outros tipos de objetos.

- Audit Policy Change: Controla as alterações feitas aos diretórios de usuários, auditoria e relações de confiança.

- Audit Privilege Use: Controla o uso de diretório e privilégios do usuário, auditoria e relações de confiança.

- Audit Process Tracking: Controla os processos de sistema e os recursos que eles usam.

- Audit System Events: Controla a inicialização, desligamento e reinicialização do sistema, alem das ações que afetam a segurança ou o log de segurança.

2.2.2 Auditoria em Nível de Organização

O log de auditoria do administrador no Microsoft Exchange Server 2010 tem a finalidade de registrar em log quando um usuário ou administrador faz uma alteração na organização. Com o log das alterações é possível rastrear quem fez alterações na organização, atender a requisitos regulamentares, se ter maior controle em gerenciar e auditar as modificações em nível global. Esse recurso permite auditar os Cmdlets que são executados diretamente no Shell de Gerenciamento do Exchange, as operações realizadas usando o EMC (Console de Gerenciamento do Exchange) e a interface de gerenciamento Web do Exchange - porque essa operação executam cmdlets em segundo plano. Os cmandlets Get- e Search- não são registrados em log. O objetivo do registro em log de auditoria é mostrar quais ações foram tomadas para modificar objetos em uma organização do Exchange, e não os objetos exibidos. (TECHNET, 2012).

Por padrão o registro em log de auditoria é configurado para armazenar entradas de log de auditoria por 90 dias, é recomendado modificar essas configurações para atender os requisitos de auditoria da organização.

2.3 Conformidade de Mensagens

As capacidades de conformidade de e-mail foram introduzidas no Exchange Server 2007 e construídas sobre troca de mensagens no Exchange Server 2010, estão focadas em conformidades regulamentares e descoberta legal. Neste contexto descoberta legal refere-se à exigência de se apresentar todas as informações relevantes a e-mail durante litigio, geralmente como resultado de uma intimação. Conformidade está relacionada a satisfazer requisitos regulamentares que podem dividir geralmente em três categorias: (JAGOTT; STIDLEY,2010).

- Regulatório: Conformidade regulamentar governamental normalmente é o que está por trás do cumprimento regulamentar. Conformidade regulatória tem sido uma preocupação predominante para os serviços financeiros e os setores de saúde, mas também tem grande importância para praticamente todos os setores públicos e privados.

- Legal: ligado aos litígios e geralmente são movidos para cumprimento de ordem jurídica.

- Interno: Conformidade interna em muitos casos se resume em mitigar os riscos para a organização. Os riscos estão inseridos nas preocupações como violação de privacidade, perdas financeiras, responsabilidades corporativa (civil ou criminal), divulgação de ativo intelectual.

Segundo Jagott e Stidley (2010), é estimado que os maiores gastos em conformidade pelas organizações estão ligados a gasto com pessoal, e que o custo global de cumprimento corre para os bilhões para alguns setores, como os financeiros e mobiliários. Os recursos fornecidos no Exchange Server 2010 podem permitir que as organizações atendam seus requisitos de conformidade com menor custo e esforço.

Para satisfazer as necessidades de uma organização no tocante ao cumprimento de conformidade de mensagens dentro do Exchange, mesmo os regulamentos variando amplamente nas mais diversas jurisdições, uma solução de conformidade no correio eletrônico pode ser atendida pelas capacidades a seguir.

2.3.1 Retenção de Mensagens

A retenção de mensagens é alcançado com a tecnologia de gerenciamento de registros mensagens (MRM). Isso permite que a organização bem como seus usuários individuais possa manter ou remover mensagens como necessário para o cumprimento da política da empresa, regulamentação governamental, ou requisito de necessidade legal, bem como para remover e-mail que não precisa ser mantido. A remoção de mensagens que não precisam ser retidas pode auxiliar no controle do crescimento de caixa e os recursos necessários para suportar esse crescimento. Quando o limite de idade para a retenção é atingida, um e-mail pode ser apagado ou arquivado, um evento pode ser logado, ou a mensagem pode ser sinalizada para atenção do usuário. (JAGOTT; STIDLEY,2010).

O MRM pode fornecer um abrangente solução de conformidade de e-mail. (JAGOTT; STIDLEY,2010). E combinam marcas de retenção, diretivas de retenção e auto-marcação. As pastas de caixa de correio e itens de e-mail individuais usam marcas de retenção para aplicar as configurações de retenção. (STANEK, 2011).

Os usuários participam no processo de MRM categorizando as mensagens de acordo com o conteúdo e requisitos de retenção. Quando o usuário não marca manualmente a mensagem, uma marca padrão associada a uma diretiva de retenção é aplicada. A auto-marcação é uma forma baseada na aprendizagem das preferências dos usuários pelo Exchange Server 2010, ele aprende as preferências de marcas do usuário e atribui marcas às mensagens de entrada automaticamente. Quaisquer marcas atribuídas automaticamente podem ser substituídas manualmente pelo usuário.

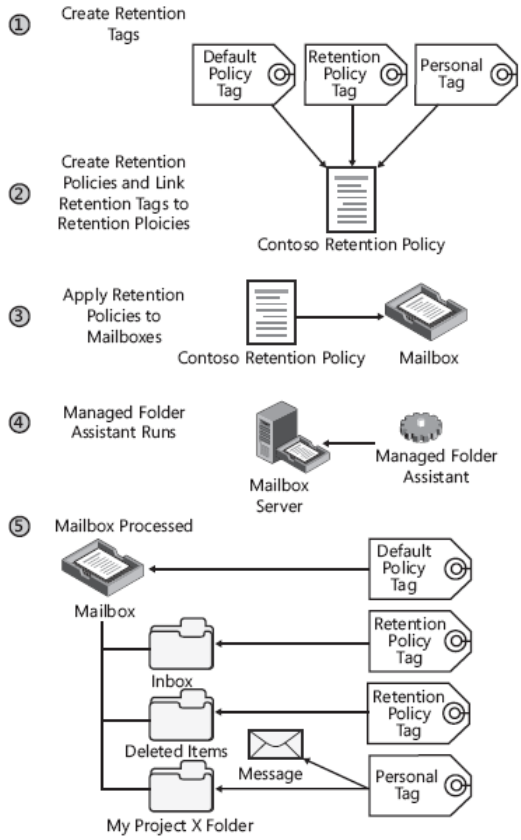
2.3.1.1 Marcas de Retenção

As marcas de retenção (retention tags) são definições de configurações de retenção que são aplicadas em pastas e ou itens individuais dentro das pastas. As configurações definem o período de retenção para o tipo de item, e qual ação a ser tomada quando a idade especificada é atingida. Quando as mensagens alcançam esse limite o Exchange Server pode manter o conteúdo das mensagens ou excluir o que for desnecessário sem precisar da intervenção do administrador. As configurações de exclusão podem excluir permanentemente o conteúdo, ou de forma que o usuário possa recuperá-lo. Pode também movê-lo para uma pasta gerenciada permitindo que o proprietário o examine antes de excluir. (STANEK, 2011).

Para implementar as marcas de retenção é necessário criar marcas de diretiva de retenção (retention policy tags - RPTs) para as pastas padrão e depois criar e aplicar as diretivas de retenção às caixas de correio. Não pode ser aplicado a itens individuais. E para trabalhar com diretivas de retenção e marcas de retenção é necessário utilizar o Exchange Management Shell. (STANEK, 2011).

A Ilustração abaixo apresenta o funcionamento da marca de retenção e política de retenção:

Figura 04: Representação de marca de retenção e política de retenção.



Fonte: Microsoft Exchange Server 2010 Best Practices (JAGOTT; STIDLEY, 2010, p. 350).

Além do listado anteriormente, uma marca de política padrão (default policy tag - DPT) pode ser criada, quando a DPT é adicionada a uma política de retenção e a mesma é atribuída a uma caixa de correio, as configurações de marcas aplicam a todas as pastas e os itens dentro da caixa de correio que não tem outras marcas atribuídas ou por meio de herança na pasta.

Pode se ter ainda as marcas pessoais (personal tags), que quando criada e adicionada a uma política de retenção os usuários cuja caixa de correio for aplicada pode marcar itens individuais ou dentro de pastas que não são padrão dentro de sua caixa com essa marca pessoal. O resultado é que as configurações definidas são aplicadas para o item ou pasta, se aplicado a um item, a marca

pessoal substitui as outras marcas que poderiam ter sido atribuídas à pasta, ou qualquer marca de política padrão aplicada a caixa de correio. Se aplicado a uma pasta não padrão, a marca substitui qualquer marca atribuída anteriormente a essa pasta. (JAGOTT; STIDLEY, 2010).

2.3.1.2 Política de Retenção

Politica de retenção são coleções de marca de retenção que é aplicada a caixas de correio para implementar configurações de retenção para itens e pasta na caixa de correio.

2.3.1.3 Retenção Legal

Retenção Legal (Retention Hold) tem o intuito de preservação imediata de itens de caixa de correio quando excluído ou editado. Aplica-se a caixa de correio primária e ao arquivo pessoal e pode ser utilizada em caso de litígio, onde se deseja preservar os dados de e-mail quanto a exclusão para preservar os dados. (STANEK, 2011). Outra utilidade é em caso de usuário ausente por logo período sem acesso a e-mail. A configuração suspende o processamento de política de retenção para a caixa de correio, impede que as mensagens sejam apagadas, ou movidas para arquivo pessoal antes que o usuário tenha a oportunidade de ler.

2.3.1.4 Gerenciamento de Descoberta

O gerenciamento de descoberta (Discovery Management) faz com que um usuário definido com a atribuição Discovery Management busque itens de caixa de correio em várias destas, incluindo e-mail, anexos, itens de calendário, tarefas e contatos, assim como arquivos protegidos por IRM. Essa pesquisa trabalha simultaneamente em caixas primárias e arquivos pessoais. O escopo da definição de atribuição determina as caixas de correio podem ser pesquisadas por um determinado usuário. As mensagens retornadas são copiadas em uma caixa de correio Discovery designada. Esse recurso é importante, pois garante a conformidade com os requisitos de pesquisa legal. Permite que colaboradores de RH devidamente autorizados, ou outros usuários devidamente autorizados pesquisem conteúdo de mensagens para fins de pesquisa interna e conformidade com a diretiva de mensagens da empresa. Com a capacidade avançada de filtragem

permite pesquisa por remetentes, destinatários, diretiva de vencimento, tamanho da mensagem, data de envio/recebimento, cc//cco e expressões comuns.

2.3.1.5 Arquivo Pessoal

Arquivo Pessoal (Personal Archivies) foi introduzido no Exchange 2010 e é uma solução integrada que fornece uma alternativa para os armazenamento pessoal (.pst), fornecendo meios para eliminar progressivamente esses arquivos ao importar as mensagens para o personal archivies. (JAGOTT; STIDLEY, 2010). Trata-se de caixa de correio adicional associada a uma caixa primária. Itens do arquivo primário podem ser descarregados automaticamente no Arquivo Pessoal, usando Diretivas de Retenção, reduzindo o tamanho e melhorando o desempenho da caixa de correio primária.

2.3.1.6 Auditoria (Journaling)

O Journaling é um agente de transporte focado em conformidade, ele processa as mensagens nos servidores com função de Hub Transport. (JAGOTT; STIDLEY, 2010). São regras e configurações que permitem guardar uma cópia de todas as mensagens que atendem a critérios específicos. O relatório é uma mensagem de correio eletrônico que inclui o tema ID da mensagem, o remetente e o destinatário da mensagem original e o anexo e um anexo contendo a mensagem original.

O Journaling armazena as informações de configuração no Active Directory onde é lido pelo agente e aplicado à base de dados apropriado. As regras usadas são compostas por três componentes:

- Interna: Aplicado a mensagens em âmbito interno enviados ou recebidos por destinatários dentro da organização.
- Externo: Define um âmbito externo e se aplica a mensagens enviadas para ou recebida de contas externas.
- Global: Tem o escopo global e atinge todas as mensagens que passam pelo Hub Transport.

2.3.2 Acesso Controlado

Capacidade de proteger a privacidade e a informação impedindo o acesso não autorizado aos dados tanto em trânsito como em repouso. Esses serviços são oferecidos no Exchange Server 2010 através da integração com o Active Directory Rights Management Services (AD RMS), regras de transporte e Transport Layer Security (TLS) para o SMTP, o TLS será abordado futuramente em técnicas criptográficas no correio eletrônico.

2.3.2.1 Regras de Transporte

As regras de transporte permite selecionar itens de mensagens e aplicar ações aquelas que atenderem as condições especificadas. Quando definida uma regra de transporte, todos os servidores com função de Hub Transport na organização selecionando a mensagem de acordo com as regras definidas. As regras de transporte têm condições, ações e exceções que podem ser aplicadas. Exemplos de condições:

- From People: Permite selecionar as mensagens de um destinatário.
- Send To People: Permite selecionar as mensagens enviadas para uma pessoa.
- When Any Of The Recipients In The to Field Is People: Permite selecionar as mensagens a destinatários específicos.

Quando uma mensagem atende a todas as condições especificadas em uma regra de transporte, a mensagem é manipulada de acordo com as ações definida. Exemplo de condições:

- Log Na Event With Message: Registra um evento em logs da aplicação com a mensagem que for especificada.
- Append Disclaimer Text: Anexa um texto de ressalva à mensagem.
- Send Bounce Message: Remove a mensagem e envia uma mensagem de não entrega para o remetente.

As regras de transporte podem ter exceções, que são semelhantes aos critérios de condições.

2.3.2.2 Regras de Proteção em Transporte

Protege o conteúdo da mensagem contra revisões e acessos não autorizados protegendo os anexos e mensagens de e-mail. A proteção e efetivada no transporte onde é aplicado configurações de direito a mensagem, determinando que destinatários podem acessar a mensagem e que ações podem ser executadas. Por exemplo o destinatário pode ter permissão de visualizar uma mensagem e anexos, mas não ter permissão de imprimi-los. Essa técnica é alcançada ao Integrar o Exchange Server 2010 com o AD RMS, que será enfatizado posteriormente.

2.3.3 Integridade da Informação e Processos

Capacidade que engloba a classificação da mensagem e processamento da mensagem com base em sua classificação. Pode também incluir parede ética para bloquear a comunicação entre departamentos específicos ou indivíduos da organização para ajudar a prevenir conflitos de interesses. Classificação de mensagem é um componente integrado no Exchange Server 2010 e paredes éticas podem ser construídas utilizando regras de transporte.

2.4 Exchange 2010 Trabalhando com AD RMS

Ao trabalhar com AD RMS (Active Directory Rightd Management Services) em uma organização do Exchange se tem uma tecnologia de proteção das informações, permiti implementar modelos de diretivas de uso que definem o uso autorizado e não autorizado, seja online, off-line, dentro ou fora do firewall. Pode assegurar a integridade dos dados gerados, proteger propriedade intelectual e controlas quem pode fazer o que com documentos gerado dentro de uma organização. Com essas propriedades pode se limitar o risco de exposição de conteúdo fora da organização, ou seja, com os direitos atribuído um usuário pode não ter permissão para imprimir, ou encaminhar e-mail de um conteúdo. Isso significa que determinadas mensagens não podem ser encaminhadas para destinatários fora da organização reduzindo a probabilidade de que um empregado irá divulgar informações da empresa seja de forma acidental, ou maliciosa.

Vários componentes interagem com o AD RMS, os principais componentes são:

- Autor: Usuário ou serviço que gera o documento protegido.
- Aplicações AD RM: Algumas aplicações podem ser habilitadas para interagir com o AD RMS e os autores podem usar essas aplicações para criar e proteger o conteúdo e os destinatários podem usá-los para ler o conteúdo protegido.
- Destinatário: O usuário ou serviço que acessa o documento.
- Servidor AD RMS: Responsável por fornecer as licenças que controlam o acesso ao conteúdo. Quando se instala o primeiro servidor AD RMS o Exchange Server cria um cluster AD RMS e podem ser adicionados outros servidores ao cluster.
- Serviço de Banco de Dados: Armazena as configurações do AD RMS e informações relacionadas.
- AD DS e Active Directory: Serviços que autentica autores e destinatários para que o Exchange Server possa aplicar os direitos apropriados para o conteúdo.

O Exchange Server 2010 integra com o AD RMS e trabalha em conjunto para prover proteção de conteúdo quando usuários enviam mensagens através de e-mail.

Os usuários habilitados para proteger o conteúdo podem utilizar o Outlook para controlar quem pode ler, copiar, imprimir e encaminhar mensagens independente de onde elas estão armazenadas. Na criação do e-mail o usuário pode limitar o que os destinatários da mensagem podem fazer com ela e essa funcionalidade não requer nenhuma componente adicional aos que estão envolvidos no sistema de entrega de mensagem no correio eletrônico.

O Exchange 2010 fornece funcionalidades adicionais, expande os cenários pelos quais usuários e administradores podem aplicar proteção para o e-mail, tanto dentro como fora da organização:

- Regra de proteção do Outlook: Permite a aplicação de um modelo RMS antes da mensagem ser enviada.

- Regra de proteção no transporte: Permite a utilização de regra de transporte para aplicar a proteção de direito de mensagens. Essa regra ajuda as organizações a aplicar uma política de conteúdo de mensagens por meio de criptografia de e-mail cessível e gestão dos direitos de acesso ao conteúdo. Quando se encaminha a mensagem o Exchange 2010 inclui o modelo não o encaminha, apenas os destinatários especificados podem decifrar as mensagens, sendo que os destinatários não podem encaminhar a mensagem para outras pessoas, copiar o conteúdo da mensagem, ou imprimir a mensagem.

- IRM no Outlook Web App: Quando esse recurso está habilitado os usuários podem usar o Outlook Web App para enviar mensagens protegidas por IRM e ler mensagens protegidas por IRM.

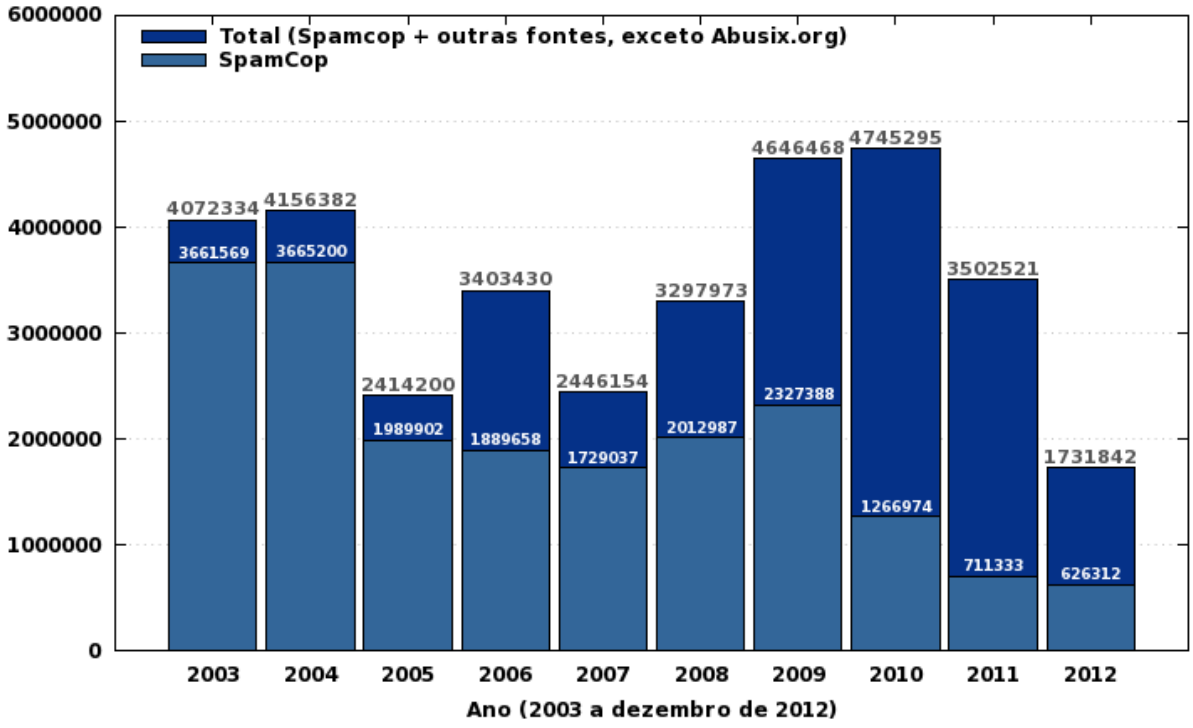
2.5 Solução ANTISPAM

O protocolo SMTP que permite o envio fácil de e-mail a qualquer servidor de e-mail no mundo é simples, mas é também inseguro. Como exemplo um servidor de correio eletrônico do domínio integracao.gov.br que recebe um e-mail da Internet encaminhado a fernando.bezerra@integracao.gov.br deve aceitar e-mails de forma anônima. E devido a forma aberta da Internet é fácil a uma pessoa mal intencionada encaminhar e-mail comercial não solicitado a qualquer servidor de e-mail da Internet, essa técnica é conhecida como SPAM. Também é fácil a falsificação de correio de modo que o correio pareça vir de uma fonte confiável (Como um Banco) fazendo que a pessoa tome uma ação, como login em uma URL falsa fornecendo as credenciais bancária, essa técnica é conhecida como phishing. Ou enviar e-mail com anexos maliciosos onde se escondem vírus que podem carregar um programa no computador que vai continuar a se espalhar (programas chamados worms). Ou carregar um programa que gera spam para enviar para a lista de contatos do usuário

(chamado de bot), ou carregar um monitoramento, ou acesso remoto no computador que um Hacker mal intencionado pode usar.

A verificação de mensagem com conteúdo inapropriado é conhecido como solução de higiene de mensagem. Na atualidade todos os sistemas de correio eletrônico devem ter algum sistema para higiene de mensagens que protejam contra vírus e reduza a quantidade de mensagens comerciais não solicitadas nas caixas de correio dos usuários. O cert.br disponibiliza uma estatística de spam reportados por ano desde 2003, nela se vê a necessidade de ter uma solução eficiente na limpeza de e-mails que circulam em uma organização.

Figura 05: Estatística de Notificações de Spam Reportadas ao CERT.br - valores acumulados: 2003 a dezembro de 2012.

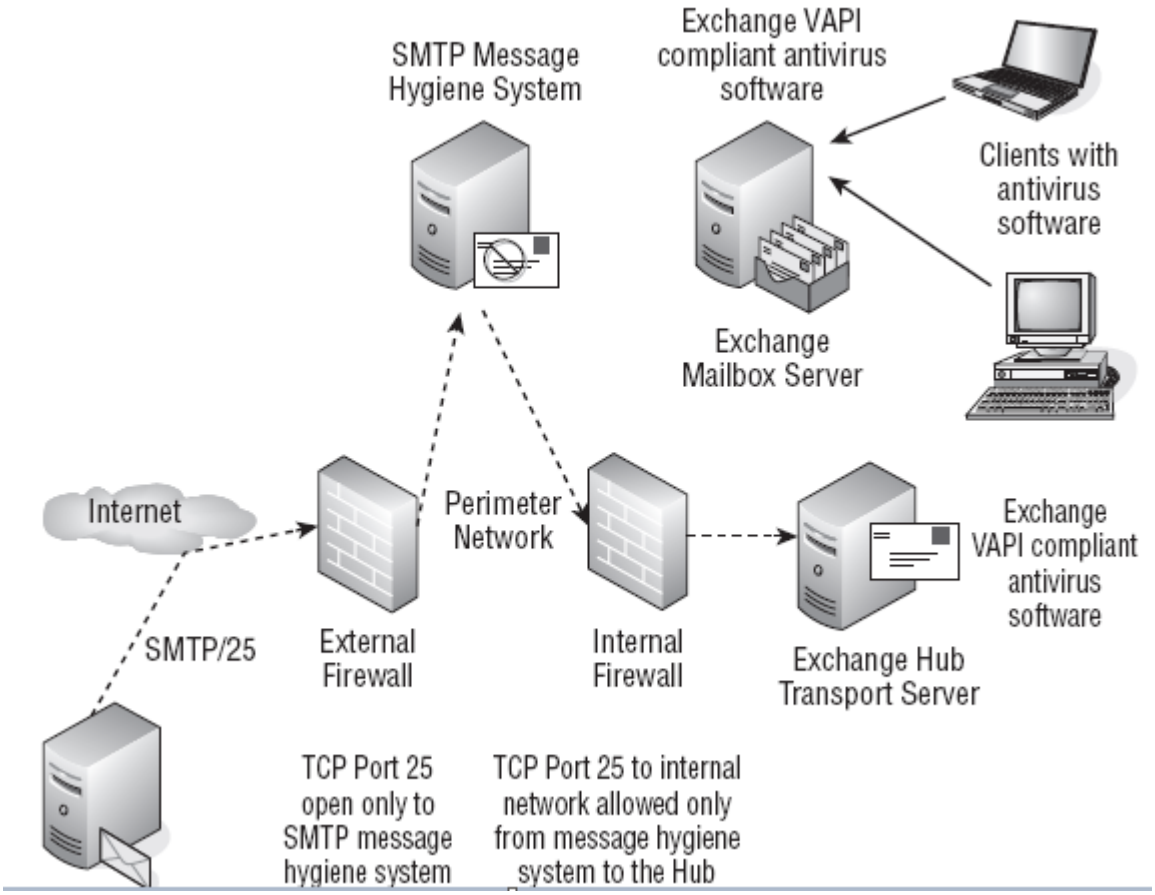


Fonte: http://www.cert.br/stats/spam/

O Exchange 2010 fornece um nível elevado de proteção contra spam por meio dos agentes ANTISPAM implantados em servidores com função de Edge Transport, esses agentes também podem ser implantados manualmente em servidores com função Hub Transport, essa função sozinha não é capaz de proteger contra vírus e deve ser introduzido um software adicional para proteção contra vírus. (MCBEE; ELFASSY, 2010).

Uma forma eficaz e eficiente de se aplicar filtro ANTISPAM e antivírus deve ser tratada em múltiplas camadas. Abaixo um exemplo de organização usando uma infraestrutura própria para a filtragem em múltiplas camadas.

Figura 06: Implementação de sistema de higienização de e-mail em múltiplas camadas



Fonte: Mastering Microsoft Exchange 2010 (MCBEE e ELFASSY, 2010, p. 135).

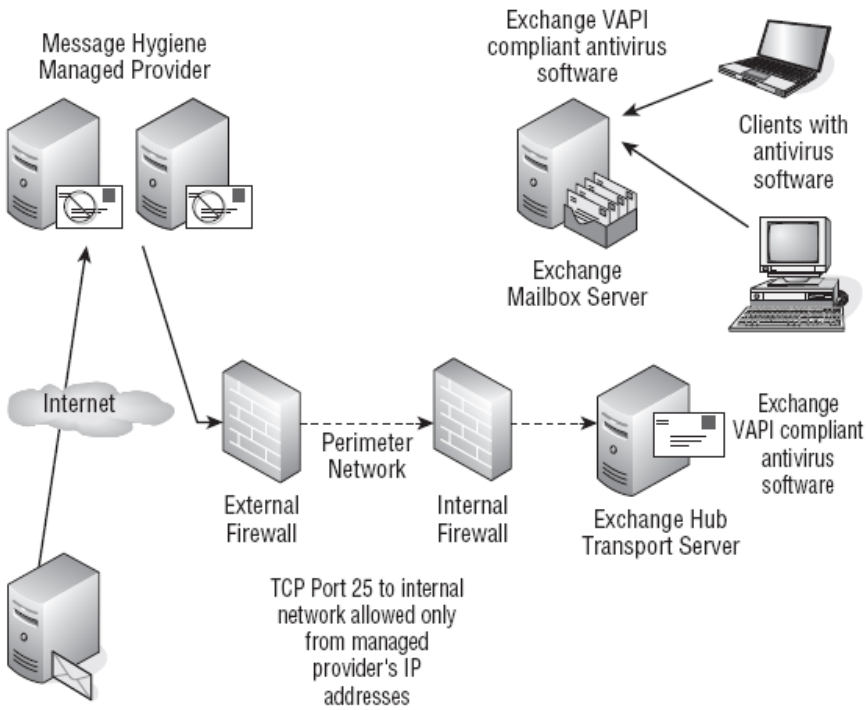
O sistema em múltiplas camadas apresenta a funcionalidade de poder parar uma ameaça em mais de um lugar. Seguindo esse raciocínio, um e-mail mal intencionado será interrompido pelo sistema de higiene de mensagens na rede de perímetro (DMZ), podendo ser uma função no Edg Transport ou ser uma solução de terceiro, (especializada em tratamento de segurança de mensagem baseado em mensagem SMTP). O conceito de sistema de higiene de perímetro tem como princípio eliminar o máximo de conteúdo indesejado antes de alcançar o sistema de produção de e-mail e para proteger os servidores de e-mail internos de possíveis tentativas de comprometê-los. (MCBEE; ELFASSY, 2010).

Depois de ser filtrada na DMZ, a mensagem é então transferida para servidores Exchange na rede interna, que devem verificar as mensagens nos servidores de transporte ou quando a mensagem é colocada na caixa de entrada do usuário. Seguindo as melhores práticas, o sistema de filtro de spam na rede interna deve ser um mecanismo diferente do utilizado na rede de perímetro. (MCBEE ; ELFASSY, 2010).

A última camada de proteção é aplica no cliente, (deve ter um sistema de verificação de arquivos e memória que deve verificar qualquer conteúdo). O ideal é que o software em execução no cliente seja de um fornecedor diferente do software executado nos servidores. A execução de software de verificação e filtragem de e-mails diferentes melhora a probabilidade de eliminar uma ameaça interrompendo sua ação. (MCBEE; ELFASSY, 2010).

Uma organização pode terceirizar a infraestrutura de higienização de e-mail, pode contratar um parceiro especializado que irá analisar as mensagens antes de ser entregue aos Servidores Exchange da organização. Abaixo um exemplo de provedor dessa solução.

Figura 07: Sistema de higienização de e-mail terceirizado

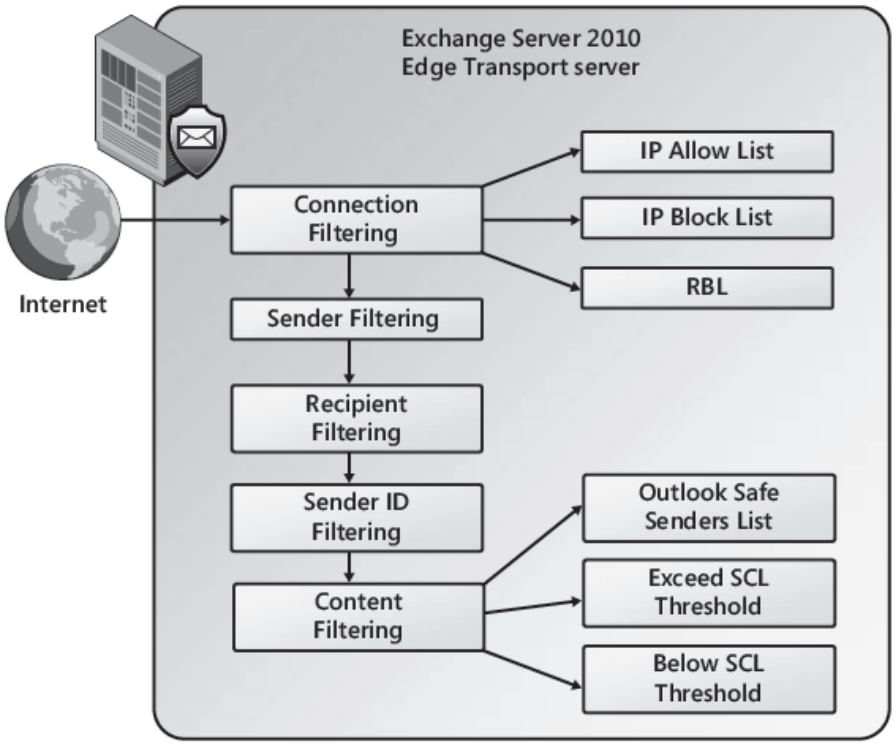


Fonte: Mastering Microsoft Exchange 2010 (MCBEE e ELFASSY, 2010, p. 136).

Pelo visto até o presente momento se constata a necessidade de perder algum tempo planejando uma solução adequada para reduzir o grande número de mensagens de spam que circulam na Internet, a verificação dessas defesas tornou-se uma das tarefas mais importante na administração de serviço de correio eletrônico. Por padrão o agente AntiSpam é instalado somente no servidor Edge Transport, contudo é uma boa prática instalá-lo em servidores com função de servidor Hub Transport e assim ter mais um ponto de inspeção. (JAGOTT; STIDLEY, 2010).

O Exchange 2010 possui uma variedade de recursos AntiSpam que trabalham cumulativamente para reduzir a quantidade de spam que entram em uma organização. Isso é proporcionado ao utilizar os agentes de filtragem de spam. Pode ser visto abaixo uma figura que representa o que acontece quando um servidor SMTP da Internet conecta a um servidor Edge Transport e inicia uma conexão SMTP, onde examina cada mensagem usando a sequência representada. (JAGOTT; STIDLEY, 2010).

Figura 08: Sequência de Agente de Filtro de Spam



Fonte: Microsoft Exchange 2010 Best Practices (JAGOTT; STIDLEY, 2010, p. 298 e 299).

2.5.1 Filtro de Conexão

O Conection Filtering (filtro de conexão) é um agente ANTISPAM habilitado nos computadores Executando a função de servidor Edge Transport. Ele se baseia no endereço IP do servidor remoto que está tentando se conectar para determinar a ação que será executada na mensagem de entrada.

Quando habilitado o agente ANTISPAM o filtro de conexão é o primeiro a ser executado quando uma mensagem de entrada é avaliada. Ele inspeciona o endereço IP do servidor remoto que tenta enviar a mensagem para definir a ação que será tomada a mensagem de entrada. Podem ser verificado da seguinte forma:

- IP Allow List - Lista de IPs Permitidos: Verifica se o servidor especificado é encontrado na lista de IP permitidos, se estiver na lista a mensagem não é processada nos demais filtros, mas enviada diretamente ao destino.

- IP Allow List Providers (Lista de Provedores de IPs Permitidos): São listas dinâmicas mantidas por provedores terceirizados, para utilizar a lista á necessário configurar um provedor externo que mantém uma lista segura de servidores SMTP, a forma de processamento é semelhante a Lista de IPs Permitidos.

- IP Block List (Lista de IPs Bloqueados): Essa lista é adicionado os servidores que são conhecidos por encaminhar mensagens de Spam e tem as mensagens bloqueadas ou assinaladas como spam.

- IP Block List Providers or real-time block lists (Provedores de lista de bloqueio de IP ou lista de bloqueio em tempo real (RBL)): As RBLs foram criadas em 1997 por Paul Vixie no projeto MAPS (Massachusetts Alliance of Portuguese Speakers). Na época este era o único serviço de bloqueio de SPAM. Consiste de uma lista de endereço IP de servidores SMTP que são considerados com risco para envio de spam. Se ativado, o agente enviará uma consulta DNS para o provedor de lista de bloqueio de IP, caso a resposta do provedor indicar que o IP da conexão está na lista, o agente irá rejeitar a operação após o comando RCPT TO:. As configurações são feitas de forma que se pode ter várias exceções no caso de um ou mais

destinatários necessitarem receber as mensagens de um servidor assinalado como servidor que envia spam. (JAGOTT; STIDLEY, 2010).

2.5.2 Filtro de Remetente

Sender Filtering (Filtro de Remetente) uma das características ANTISPAM mais antiga e provavelmente a menos eficaz. Tem como conceito a inserção de endereços SMTP ou domínios que não podem ser capaz de enviar e-mail para usuários da organização. O que torna essa técnica ineficaz é o fato de spammers em sua maioria não usarem a mesma abordagem ou o mesmo e-mail duas vezes.

Ele Compara o remetente no MAIL FROM: a uma lista de remetentes ou remetentes de um domínio que são proibidos de enviar mensagens para a organização. Após ser filtrado pode se ter duas ações: rejeitar a mensagem ou carimbá-la e encaminhar para frente para continuar a serem tratados pelos demais filtros. (JAGOTT; STIDLEY, 2010).

2.5.3 Filtro de Destinatário

Quando ativado a filtragem de destinatário (Recipient Filtering) é rejeitado os e-mails destinados a qualquer endereço SMTP que não está no Active Directory ou para rejeitar e-mail destinado a endereço SMTP especifico. É recomendado bloquear as mensagens enviadas aos destinatários não incluídos no diretório, pois isso diminui a carga nos servidores e inibe o encaminhamento de relatórios de não entrega. (MCBEE; ELFASSY, 2010).

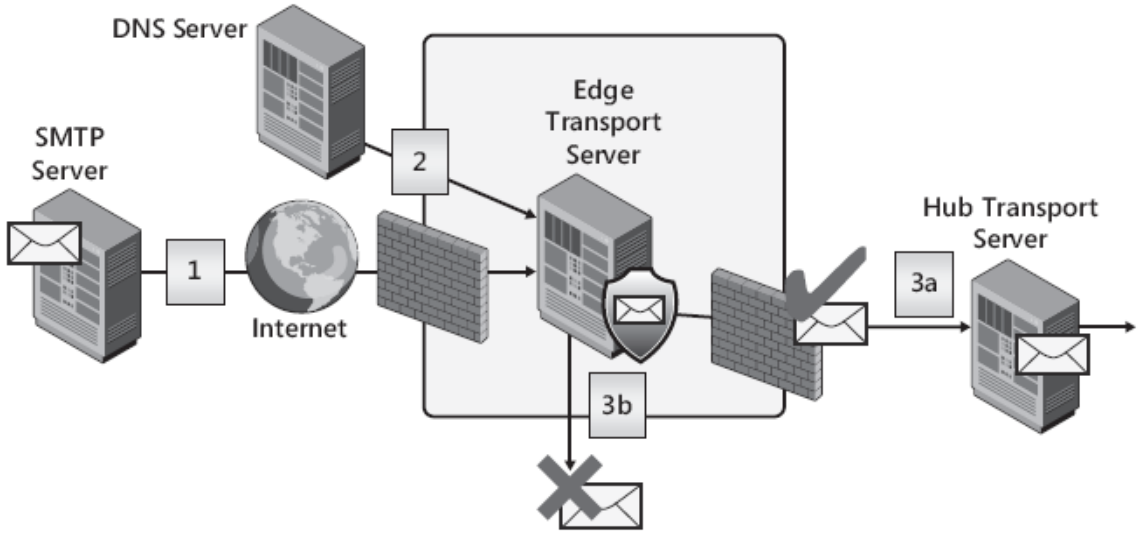
No processo são comparados os destinatários da mensagem sobre o comando SMTP no RCP TO: no caso de ser encaminhado a mais de um e-mail e um não fazer parte do diretório, ou estiver definido na lista de endereço especifico, a mensagem não será entregue ao destinatário especificado na lista de bloqueio de destinatário, mas será entregue aos outros destinatários que não estão na lista e fazem parte do diretório do Active Directory.

2.5.4 Filtragem por ID do Remetente

O Sender ID Filtering (Filtragem por ID do Remetente) é um padrão da indústria que permite que as empresas verifiquem os endereços IP para mensagens recebidas para garantir que eles vêm de servidores autorizados. O Sender ID Framework fornece proteção altamente eficaz contra falsificação de domínio de e-mail e esquema de Phishing. No entanto, sender ID não é usado por muitas grandes empresas. O conceito é que os proprietários de domínios devem registrar todos os endereços IP de todos os servidores SMTP que são autorizados a encaminhar e-mail em nome do domínio como registros especiais no DNS. (JAGOTT; STIDLEY, 2010).

Com o Sender ID Filtering o servidor de mensagem destinatário inicia uma pesquisa DNS para verificar se o IP de conexão é permitido para entregar mensagens em nome do domínio. Se a informação de domínio não tem o enderço IP do servidor de conexão, as mensagens podem ser filtradas. Abaixo uma ilustração e explicação de como o Sender ID Filtering trabalha. (JAGOTT e STIDLEY, 2010). Como ele se baseia no domínio do remetente da mensagem torna mais difícil para os Spammers enviarem SPAM, já que em muitos casos os Spammers forjam endereços de e-mail de remetentes para encaminhar SPAM.

Figura 09: Como o Send ID Filtering Trabalha



Fonte: Microsoft Exchange 2010 Best Practices (JAGOTT; STIDLEY, 2010, 2010, p. 322).

Explicação da figura:

- 1 - A mensagem é recebida da Internet sendo entregue ao servidor com Função de Edge Transport.
- 2 - O Servidor Edge Transport verifica o endereço IP do servidor SMTP que está enviando a mensagem com uma consulta DNS verificando se o servidor SMTP é um endereço válido para entrega de e-mail em nome da organização no registro spf.
- 3a - Se o registro corresponder ao servidor SMTP de envio, o servidor Edge Transport aceita a mensagem.
- 3b - Se o registro não corresponder, o servir Edge Transport prosseguirá conforme a definição configurada podendo rejeitar a mensagem, excluir ou encaminhar a mensagem com a informação adicional adicionada ao cabeçalho da mensagem indicando que a autenticação falhou.

Para desfrutar das vantagens do sender ID Framework e proteger a reputação da organização, deve ser criado uma identificação de remetente, ou registro SPF e adicioná-lo nos servidores DNS. O registro é um único registro de texto (TXT) no banco de dados do DNS que identifica cada servidor de e-mail autorizado a encaminhar e-mail em nome do domínio. Registros sendes ID podem usar vários formatos, como exemplo os registros SPF da figura abaixo.

Figura 10: Exemplo de Configuração de Registro SPF

DNS CONFIGURATION	DESCRIPTION
`Litware.com. IN TXT "v=spf1 mx -all"`	This record indicates that all servers that have an MX record for the Litware.com domain are allowed to send messages.
`Litware.com IN TXT "v=spf1 ip4:10.10.0.20 -all"`	This record indicates that only the server with the IP address 10.10.0.20 is allowed to send messages for Litware.com.
`Litware.com IN TXT "v=spf1 a -all"`	This record indicates that any host with an A record can send mail.
`Litware.com IN TXT "v=spf1 mx mx:berlin-et01 .emea.litware.com mx:berlin-et02.emea .litware.com -all"`	This record indicates that only the listed servers are allowed to send messages for Litware.com.

Fonte: Microsoft Exchange 2010 Best Practices (JAGOTT; STIDLEY, 2010, p. 323).

2.5.5 Filtragem de Conteúdo

O agente filtragem de conteúdo (Content Filtering) usa tecnologia SmartScreen para analizar uma mensagem e informar se é SPAM. No Exchange essa tecnologia é nomeada de FMI (Intelligent Message Filter) e o filtro de conteúdo usa o Microsoft Exchange serviço de atualização AntiSpam para atualizar os filtros. Após uma mensagem ser recebida é verificado o conteúdo com padrões reconhecíveis e é atribuída uma classificação com a probabilidade que a mensagem seja um spam. (JAGOTT; STIDLEY, 2010). A classificação é anexada a mensagem com um SCL, que é um valor entre -1 e 9:

- -1: Mensagem atribuída de uma fonte confiável.
- 0: Mensagem categorizada como não spam.
- 1 – 4: Mensagem com probabilidade extremamente baixa de ser spam.
- 5 – 9: Mensagem com probabilidade extremamente alta de ser spam.

Por padrão os servidores com função de Edge Transport que foi habilitado a função de filtragem de conteúdo é configurado para rejeitar todas as mensagens com classificação SCL igual ou superior a sete, mas essas configurações podem ser modificadas pelo administrador para rejeição, quarentena ou para apagar mensagem no fluxo de entrada. Essa classificação pode ser visualizada no cabeçalho da mensagem. (JAGOTT; STIDLEY, 2010).

2.5.6 Filtro de Reputação do Remetente

Filtro que toma as decisões com base em informações sobre recentes e-mails recebidos de um remetente específico. O agente de reputação do remetente analisa várias propriedades a respeito do remetente do e-mail para criar um nível de reputação do remetente (SRL). O SLR é um número que varia de 0 a 9, sendo que 0 indica menos que um por cento de chance de ser um remetente de spam e um valor de 9 indica mais de 99 por cento de chance de ser um remetente de spam. No caso do remetente parecer um encaminhador de spam o agente de SLR adiciona o endereço IP do servidor SMTP que está enviando a mensagem para a lista de bloqueio de IP. (JAGOTT; STIDLEY, 2010).

Quando é recebido o primeiro e-mail de um remetente, o remetente SMTP é atribuído um SRL igual a 0. Se mais mensagens chegarem do mesmo remetente o agente de reputação do remetente avalia a mensagem e começa a ajustar a avaliação do remetente. São usados os seguintes critérios para avaliação:

- Teste para verificar se o remetente não é um servidor proxy aberto.
- Analise HELO/EHLO.
- Pesquisa de DNS Reverso.
- Análise de classificação SCL da mensagem.

2.5.7 Filtragem de Anexos

É uma forma de se escolher os formatos de arquivos que os usuários da organização podem receber. Os anexos recebidos por usuários de correio eletrônico podem ser ameaças que expõem a segurança de toda a rede, como exemplo, um dos vírus mais famoso da história de mensagens, o vírus Melissa, que foi espalhado com um anexo malicioso. Os anexos obviamente perigosos como scripts ou executáveis são removidos. A filtragem de anexos é um recurso que só está disponível em servidores com função de Edge Transport, mesmo que sejam instalados os agentes ANTISPAM em servidor com função de Hub Transport o recurso não será habilitado. (JAGOTT; STIDLEY, 2010).

A filtragem de conteúdo pode ser baseada nos seguintes critérios:

- Nome do Arquivo, ou extensão do arquivo.
- Tipo de conteúdo MIME do arquivo.

Caso os critérios configurado sejam detectados em uma mensagem o agente de filtragem de conteúdo pode tomar as seguintes ações:

- Remover o anexo e entregar a mensagem ao destinatário.
- Bloquear a mensagem na entrada do sistema, gera um relatório que é encaminhado ao remetente informando que a mensagem tinha um conteúdo impróprio que não pode ser aceito a entrega.

- Apagar silenciosamente a mensagem, isso exclui a mensagem antes de entrar no sistema, mas não gera nenhum relatório informando o remetente que a mensagem não pode ser entregue.

2.6 Utilização de Técnicas Criptográficas

Segurança em mensagens, baseada em criptografia, podem ser separadas em três níveis: baseada em rede, baseada em sessão SMTP e baseada em cliente.

2.6.1 Segurança Baseada em Rede

Basicamente protege a comunicação no nível de rede usando protocolos como IPsec ou VPN.

O IPsec fornece um conjunto de extensões para o protocolo IP Básico e é utilizado para criptografar comunicação entre servidores. O IPSEC trabalha na camada de transporte e aplicações como o Exchange 2010 não precisa estar ciente do IPsec, geralmente é utilizado para comunicação servidor a servidor, ou cliente a servidor e quando está utilizando comunicações IPsec não é necessário utilizar outro método de criptografia.

VPN (Virtual Private Network também opera na camada de transporte e é utilizada para conexões site-to-site ou client-to-site. IPsec e VPN por atuarem na camada de transporte podem ser mais vantajosos se comparado a protocolos de camada de aplicação como o S/MIME (Secure MIME).

2.6.2 Segurança Baseada em Sessão

O Exchange 2010 usa o TLS (Transport Layer Security) como protocolo padrão para criptografar comunicação entre servidores. É usado um certificado de máquina ou pode ser usado o certificado auto assinado que é criado quando se instala o servidor. O certificado auto assinado é utilizado por padrão de comunicação entre dois servidores Hub Transport, ou entre servidores Hub Transport e Edge Transport.

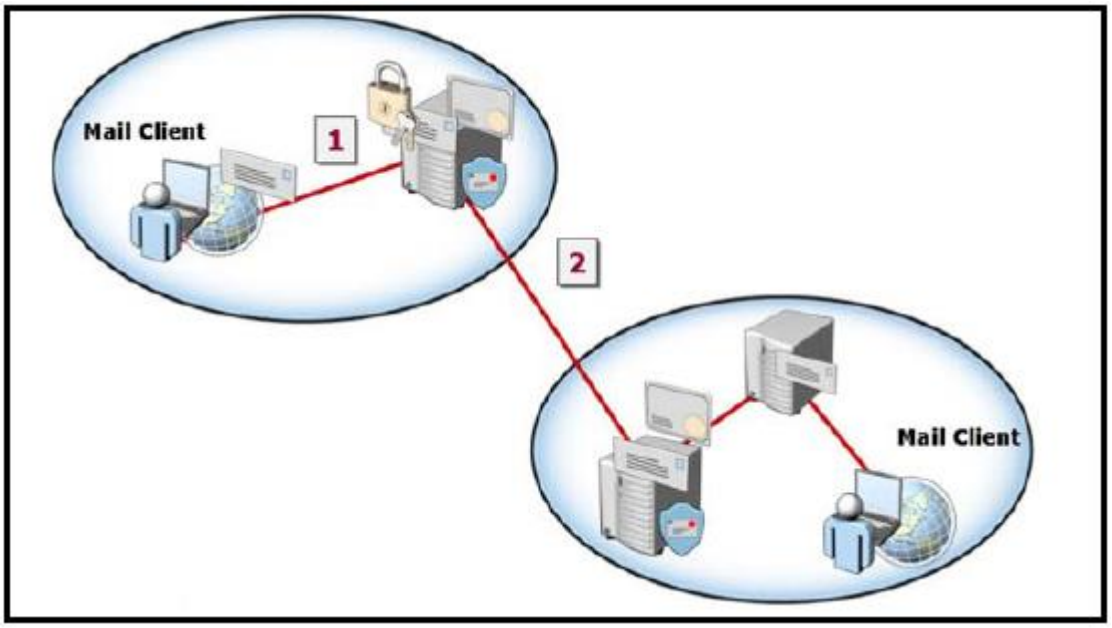
Se necessário for necessário segurança de domínio para fornecer um caminho seguro de mensagens na internet é necessário um certificado válido

emitido por uma CA Confiável. O Domínio de Segurança usa TLS com autenticação mútua, esse padrão TLS é usado para garantir a confidencialidade, criptografando, mas não autenticando os parceiros de comunicação.

O Domínio de Segurança no Exchange 2010 é usado como uma alternativa de custo mais baixo que o S/MIME e outras soluções de criptografia. Ele usa TLS mutuo para fornecer autenticação baseada em sessão de autenticação e criptografia. A autenticação TLS mútua difere da TLS normal, no TLS normal o cliente verifica se a conexão é segura ao se conectar ao servidor de destino ao validar o certificado do servidor, sendo recebida como parte da negociação TLS. Nesse cenário, o cliente autentica o servidor antes de transmitir os dados. Mas o servidor não autentica a sessão com o cliente.

Na autenticação TLS mútua, cada servidor verifica a conexão com o outro servidor, validando um certificado que é fornecido pelo outro servidor. o processo pode ser visualizado na figura abaixo:

Figura 11: Como Domínio de Segurança Trabalha



Fonte: 10135A Configuring, Managing and TroubleShooting Microsoft Exchange Server 2010 (MICROSOFT OFFICIAL COURSE, 2010, p.324)

Geralmente é configurado domínio de segurança entre organizações parceiras e as seguintes etapas devem ser seguidas antes da sua implementação:

- 1 - Solicitar e instalar um certificado no servidor de transporte em que se deseja ativar TLS mútua.
- 2 - Verificar que o TLS está funcionando dos dois lados.
- 3 - Configurar domínio de segurança de entrada e saída.
- 4 - Fazer os teste de mailflow.

2.6.3 Segurança Baseada em Cliente

O Secure Multimedia Internet Mail Extensions (S/MIME) é uma solução de segurança de e-mail SMTP baseada em cliente. O S/MIME é um padrão de criptografia de chave pública e assinatura de mensagens de e-mail. A criptografia protege o conteúdo da mensagem para que somente o destinatário possa ler. Ao assinar uma mensagem o remetente atesta que ele encaminhou a mensagem e o destinatário pode verificar se a mensagem foi alterada no caminho.

Ao contrário dos outros protocolos de criptográficos vistos, o S/MIME garante que a mensagem continue assinada ou criptografada dentro da caixa de correio e mesmo os administradores do serviço de correio eletrônico não podem decifrá-los se o certificado digital utilizado não permitir. Utilizar S/MIME oferece os seguintes recursos:

- Utilização de assinatura digital como uma forma de provar que o conteúdo da mensagem não foi modificado no meio do caminho.
- Autenticar mensagens.
- Criptografar mensagem para evitar divulgação do conteúdo.

2.7 Alta Disponibilidade

Disponibilidade em ambiente de mensageria é a porcentagem de tempo que o serviço está disponível. Como Exemplo, um ambiente que tem SLA contratado de 99,9% durante um período de um ano, de 24 horas por dia e 7 dias por semana tem um Downtime (Tempo de Inatividade) permitido de 8h45min. Abaixo figura com tempo de inatividade por ano baseado na disponibilidade desejada.

Figura 12: Inatividade Permitida para Específico Alvo de Disponibilidade

Disponibilidade Desejada	Tempo de Inatividade por Ano
99%	87h36min
99.9%	8h46min
99.99%	52min34sec
99999%	5min15sec

Fonte: elaborado pelo autor do trabalho.

Para alcançar o alvo de disponibilidade em uma organização o Exchange Server 2010 dispõe de vasta opção de alta disponibilidade (HA) que combinando com o Windows Server 2008R2 pode ser utilizado um sistema de correio eletrônico em redundância, balanceamento de carga, e Cluster de servidores. Alguns administradores conhecem bem os recursos de redundância proporcionados com a configuração de Database Availability Group (DAG), mas as funcionalidades de HA no Exchange Server 2010 vão muito além dos recursos proporcionados pelo DAG.

Foi visto anteriormente que o Exchange Server 2010 possui quatro funções principais para o ambiente de mensageria: Client Access, Hub Transport, Mailbox Server e Edge Transport e deve ser pensado redundância com base em cada função de servidor para proporcionar um ambiente de mensageria totalmente seguro e com alta disponibilidade.

2.7.1 Alta Disponibilidade no Mailbox Server

Banco de dados de caixa de correio e os dados que nele são armazenados são um dos componentes mais críticos em um ambiente de mensageria e quando se fala de redundância no Exchange 2010 o conceito mais difundido é o DAG. DAG é componente base da estrutura de alta disponibilidade e resiliência de site, recurso poderoso, provê redundância em caso de falha de uma base de dados ativa em um servidor. Cada base de dados pode ter até 16 cópias

distribuídas entre servidores Mailbox. A arquitetura de alta disponibilidade também fornece recuperação simplificada de várias falhas (nos níveis de disco, servidor e datacenter), fornecendo redundância completa dos serviços de dados do Exchange. (TECHNET, 2012).

Os grupos de disponibilidade de banco de dados permitem agrupar os bancos de dados logicamente de acordo com os servidores que hospedam um conjunto de banco de dados. Torna-se um limite de replicação de banco de dados de caixa de correio permitindo alternância de servidor e failover. Os servidores em um DAG podem hospedar outras atribuições (Roles) do Exchange e os servidores membros devem estar em um mesmo domínio do Active Directory. O Exchange 2010 melhorou a replicação contínua e substituiu os recursos de clustering do Exchange 2007 por uma solução mais robusta que não requer hardware caro e requer menos manutenção. (STANEK, 2011).

> Nas versões anteriores, o Exchange era uma aplicação clusterizada que usava o modelo de gerenciamento de recursos de cluster para alta disponibilidade. O Exchange 2010 não é clusterizado e não usa o recurso de modelo de cluster para alta disponibilidade. Em vez disso, o Exchange 2010 usa seu próprio modelo interno de alta disponibilidade. Embora alguns componentes do Windows Failover Clustering ainda sejam usados, esses componentes agora são gerenciados exclusivamente pelo Exchange 2010. (STANEK, 2011,p.304).

O Exchange 2010 inclui um novo componente chamado Active Manager, é ele que oferece as funcionalidades que substituem os recursos de cluster em versões anteriores do Exchange. Ele é executado em todos os servidores com função de servidor Mailbox membros de um DAG. Existem duas funções de Active Manager, o principal (PAM) e o em espera (SAM). O PAM decide quais cópias em um DAG será ativo e passivo, ele é responsável por obter notificações de alteração de topologia e reagir a falhas do servidor. O Membro que hospeda a função PAM é sempre o membro que atualmente possui o recurso de quorum de falhas do cluster e controla todo o movimento de designações ativas entre as cópias de base de dados - apenas uma cópia pode estar ativa, podendo estar montada ou desmontada. (TECHNET, 2012).

O SAM fornece informações sobre qual servidor hospeda a cópia ativa de uma base de dados para outros componentes do Exchange que estão executando um componente do cliente do Active Manager. Detecta falhas de armazenamento de

base de dados locais e armazenamento de informações locais. Sua reação a falha é uma solicitação ao PAM para iniciar um failover. (TECHNET, 2012).

O serviço de replicação do Microsoft Exchange monitora a integridade dos bancos de dados montados e também monitora o ESE (Extensible Storage Engine) para qualquer erro ou falha de entrada e saída. Quando detectado um erro o Active Manager é notificado. (TECHNET, 2012).

2.7.1.1 Gerenciamento de Grupo de Disponibilidade

Os grupos de disponibilidade de banco de sados são um contêiner no Active Directory e uma camada lógica na parte superior do Windows Clustering. Para estabelecer um grupo de disponibilidade e torná-lo operacional é necessário:

- Criar um grupo de disponibilidade de banco de dados.
- Adicionar servidores membros ao grupo.
- Designar servidor witness (testemunha).
- Criar uma rede de grupo de disponibilidade.

Somente membros do grupo Organization Management podem criar grupos de disponibilidade de banco de dados. E o servidor witness se faz necessário para manter o quorum quando se tem um número par de membros no grupo. Para atender os requisitos o servidor witness precisa: (STANEK, 2011).

- O servidor witness não pode ser um membro do grupo de disponibilidade de banco de dados.
- Ele deve estar na mesma floresta do grupo de disponibilidade de banco de dados.
- E deve estar em servidor com sistema operacional Windows Server 2003, ou Windows Server 2008, ou posterior.

A Microsoft recomenda usar um servidor Exchange 2010 para hospedar o diretório witness, como preferência um servidor Hub Transport no mesmo site do

Active Directory da maioria dos membros do grupo de disponibilidade de banco de dados.

Ao configurar o grupo de disponibilidade de banco de dados o Exchange cria um objeto msExchMDBAvailabilityGroup e objetos correspondentes no Active Directory. Eles representam o grupo de disponibilidade, seus membros, redes e atributos. o Objeto é usado para armazenar informações sobre o grupo de disponibilidade de banco de dados, como informações de servidor membro.

Quando o primeiro servidor Mailbox é adicionado a um grupo de disponibilidade de banco de dados ocorre o seguinte:

- O componente Windows Failover Clustering e as ferramentas de gerenciamento correspondentes são instalados.
- O cluster de failover é criado com o nome do DAG e para fins de autenticação e permissões de acesso é representado por uma conta de computador criado no container padrão de computadores, é uma boa prática movê-la para a OU em que fica os servidores Exchange.
- O servidor é adicionado ao objeto msExcMDBAvailabilityGroup no Active Directory.
- Ao criar o DAG um endereço IP é atribuído ao grupo. Quando adicionado o primeiro servidor ao grupo, o nome e o endereço IP do DAG são registrados no Domain Name System (DNS) usando um registro Host (A).
- O banco de dados do cluster é atualizado com o nome dos banco de dados que estão montados no servidor.
- É examinado as configurações de rede atual e caso a máquina tenha dois dispositivos de interface de rede é configurado para criar redes de replicação e de transmissão de mensagem separadamente.
- Diretório witness e compartilhamento de arquivo witness é criado.

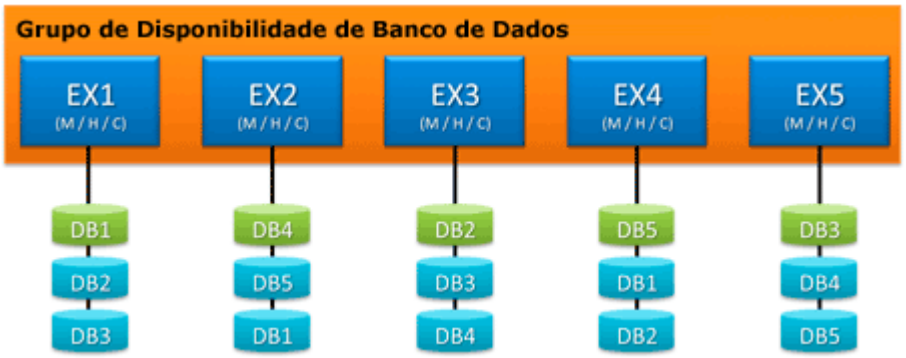
Segue o que ocorre quando se adiciona o segundo servidor e servidores subsequentes ao DAG:

- O servidor se une ao cluster de failover.
- O servidor é adicionado ao objeto msExchangeMDBAvailabilityGroup no Active Directory.
- O banco de dados é atualizado com informações dos bancos de dados que então montados no servidor.

2.7.1.2 Funcionamento de Alta Disponibilidade no DAG

Para ilustrar como um DAG pode fornecer alta disponibilidade são apresentadas figuras explicativas de como pode ser projetado o grupo de disponibilidade de banco de dados e como ele garante a alta disponibilidade das bases de dados do DAG.

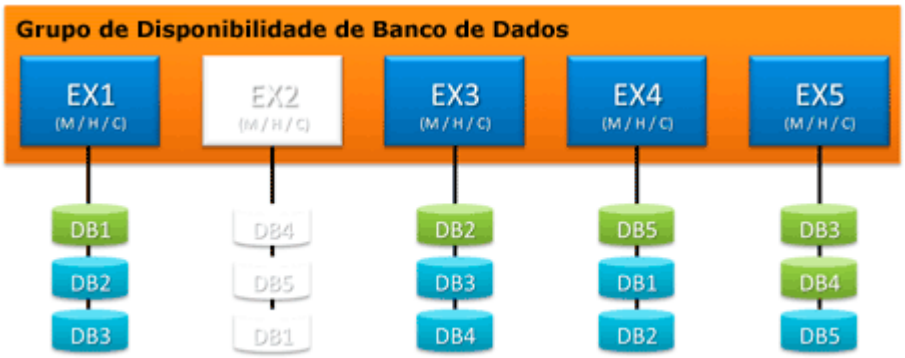
Figura 13: Grupo de Diasponibilidade de Banco de Dados



Fonte: (TECHNET, 2012).

Na figura as bases de dados (DB) em verde são cópias ativas e em azul as cópias passivas, no exemplo as bases de dados não estão espelhadas por cada servidor, mas distribuída entre vários servidores, permitindo que não exista no DAG dois servidores com o mesmo conjunto de cópias de banco de dados, fornecendo maior resiliência a falhas. (TECHNET, 2012).

Figura 14: Grupo de Diasponibilidade de Banco de Dados com um Servidor Offline para Manutenção.



Fonte: (TECHNET, 2012).

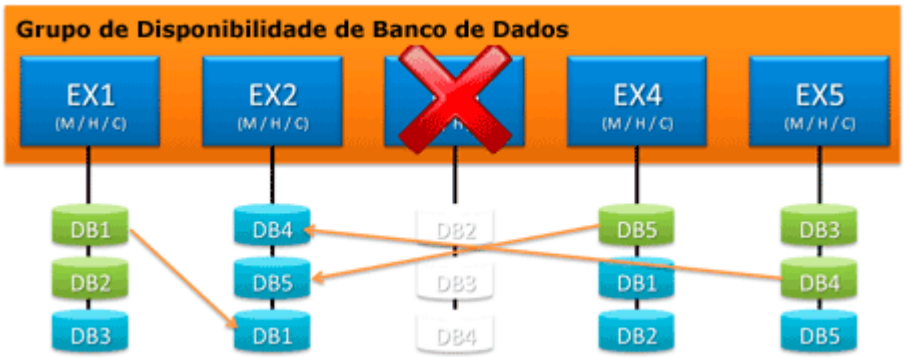
No exemplo acima um servidor foi colocado off-line, por motivo de manutenção, o administrador usou o comando Move-ActiveMailboxDatabase –Server EX2. O servidor hospedava uma cópia ativa e com o comando o próprio sistema escolhe a melhor cópia para que seja a nova cópia ativa da base de dados, no caso foi ativado no servidor EX5. No momento da manutenção o servidor EX3 passa por uma falha de Hardware, figura abaixo, e fica off-line. Como verificado na figura acima o servidor estava com o DB2 ativo que é movido para o servidor EX1 ilustrado na figura abaixo. (TECHNET, 2012).

Figura 15: Grupo de Disponibilidade de Banco de Dados com um Servidor Off-line para Manutenção e um servidor com falha.

Fonte: (TECHNET, 2012).

Após terminar a manutenção e ser colocado on-line o sevidor EX2 e estiver em funcionamento, os outros membros do DAG são notificados e as cópias que estão hospedadas no servidor EX2 começam a ser ressincronizadas com as cópias ativas de cada banco de dados. Abaixo ilustração da ressincronização.

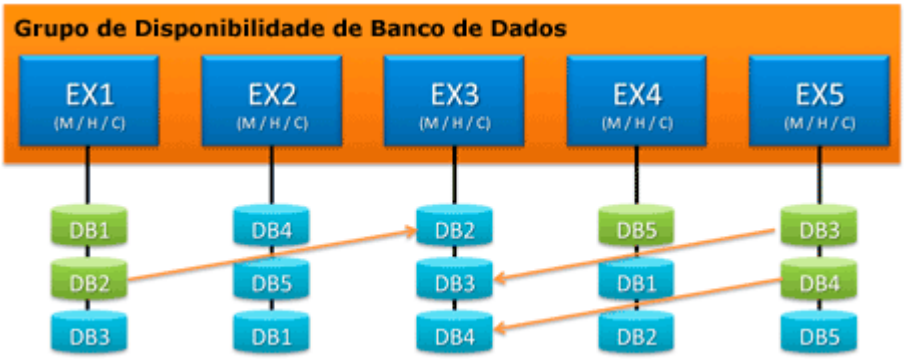
Figura 16: Grupo de Disponibilidade de Banco de Dados com um Servidor Restaurado Ressincronizando as Cópias de Banco de Dados



Fonte: (TECHNET, 2012).

Após serem resolvidos os problemas de Hardware no servidor EX3 e o mesmo estiver on-line os outros membros do DAG são notificados e suas cópias de banco de dados são automaticamente ressincronizadas com a cópia ativa de cada banco de dados, ilustração abaixo.

Figura 17: Grupo de Disponibilidade de Banco de Dados com um Servidor Reparado Ressincronizando Suas Cópias de Banco de Dados.



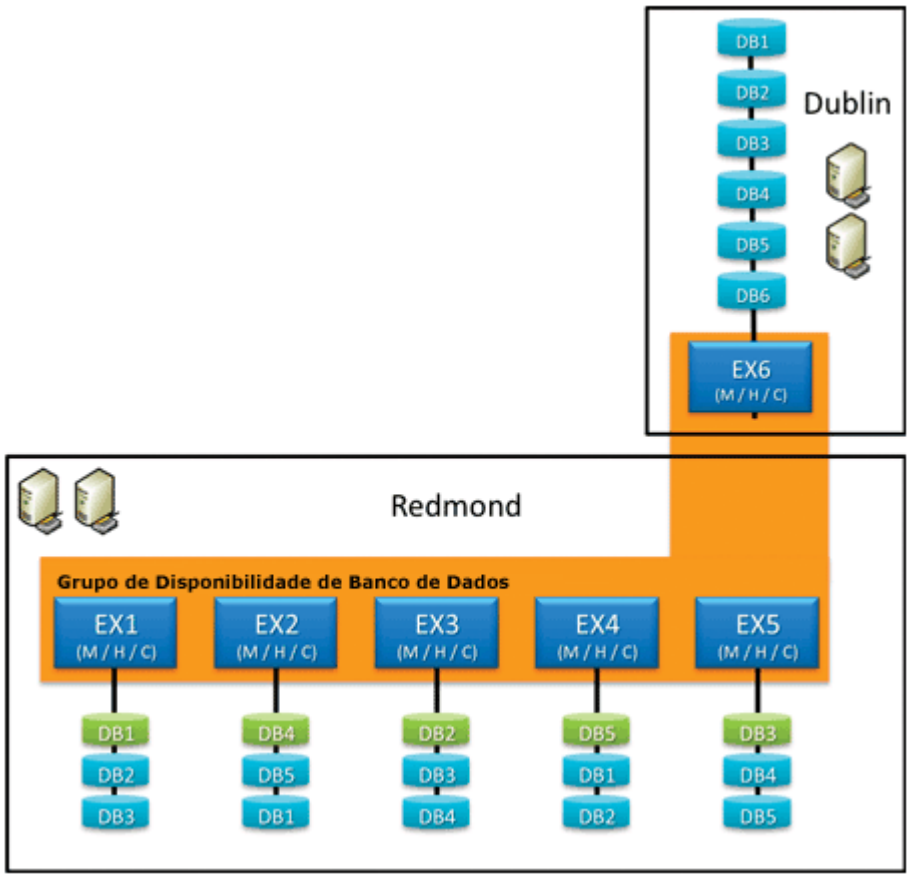
Fonte: (TECHNET, 2012).

2.7.1.3 DAG para Resiliência de Site

Com os recurso do DAG pode se estender a alta disponibilidade além de um Data Center sendo estendido para um ou mais outros data centers. Essa configuração fornece resiliência de site. Nas figuras anteriores era oferecido alta disponibilidade a um Data Center e um único site do Active Directory. Com uma infraestrutura incremental pode ser planejada para estender o DAG para um

segundo Data Center. No exemplo abaixo uma cópia passiva de cada banco de dados ativo foi configurada no servidor EX6 no Data Center de Dublin.

Figura 18: Grupo de Disponibilidade de Banco de Dados Estendido por Dois Sites do Active Directory.



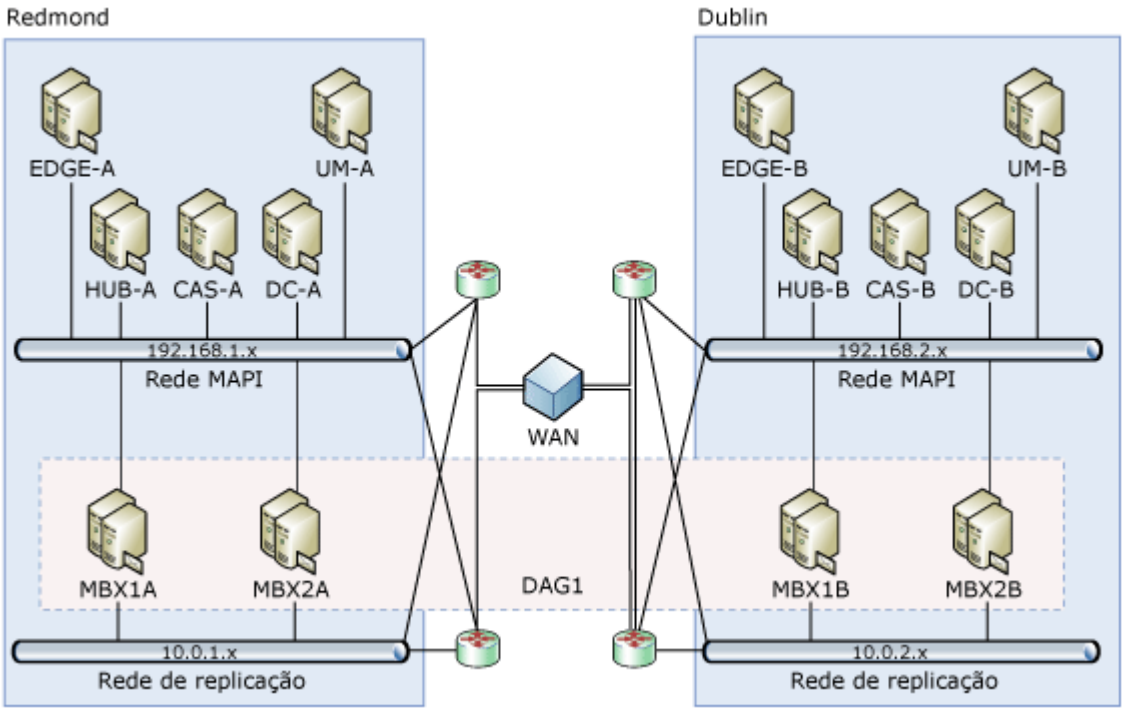
Fonte: (TECHNET, 2012).

Para se estender o grupo de disponibilidade por dois sites necessita de uma infraestrutura que tenha notadamente os seguintes componentes:

- Serviço de diretório (Active Directory ou Serviços de Domínio do Active Directori Domain Services (AD DS)).
- Resolução de nomes DNS.
- Um ou mais servidores Client Access..
- Um ou mais servidores Hub Transport.
- Um ou mais servidores Mailbox.

Abaixo uma infraestrutura recomendada seguindo as melhores práticas Microsoft.

Figura 19: Exemplo de Grupo de Disponibilidade de Banco de Dados Estendido em Dois Sites.



Fonte: (TECHNET, 2012).

2.7.2 Alta Disponibilidade no Client Access Server

O Servidor Client Access não tem funcionalidade de alta disponibilidade embutida nele como acontece com o Servidor Mailbox. Não há um mecanismo integrado fornecendo balanceamento de carga e failover se um servidor estiver indisponível. Mas tem uma variedade de produtos que preenchem essa necessidade. Para alcançar alta disponibilidade é necessário instalar mais de um servidor Client Access no mesmo site do Active Directory. E tem três tipos de tráfego que precisam ser balanceado:

- Tráfego de redes internas.
- Tráfego de redes externas (Internet).
- Tráfego de outros servidores Client Access (proxy)

Alguns protocolos necessitam de comunicação Stateful na troca de mensagens, ou seja, a aplicação requer que a comunicação seja mantida com o mesmo servidor o tempo todo até que a comunicação seja concluída. Outros protocolos são apátridas. No caso de múltiplos servidores de balanceamento de carga, afinidade é um mecanismo para direcionar as chamadas subsequentes para o host que respondeu a solicitação inicial. O Servidor Client Access utiliza uma série de protocolos para balancear carga, incluindo o HTTP e RPC. Sendo assim o Client Access utiliza protocolos que requerem afinidade e outros que não.

2.7.2.1 Balanceamento de Carga em Servidores Client Access

Para reduzir custos e complexidade deve ser selecionada uma solução única para balanceamento de carga que funcione para cada tipo de tráfego. O mercado dispõe de um grande número de tecnologias de balanceamento de carga e deve levar em consideração os seguintes aspectos ao escolher uma tecnologia a ser incorporada em servidores Client Access:

- Funcionalidades - O Balanceador de carga tem características que vão ser usados agora, ou serão necessário no futuro.
- Gerenciabilidade - A solução é fácil de configurar e gerenciar.
- Detecção de Failover - A solução suporta detecção avançada, ou trabalha com ping simples.
- Afinidade - Quais opções a solução dispões para manter as conexões de clientes e fazer voltar ao mesmo host.
- Custo - Quanto vai custar para implementar a solução.
- Escalabilidade - Como vai se comportar a solução com o aumento de hosts.

O balanceamento de carga pode ser classificado em quatro categorias: Software Load Balances, Hardware Load Balances, Intelligent Firewall e Round Robin DNS. Será visto como utilizar cada categoria em um ambiente Exchange 2010 com alta disponibilidade.

- Software Load Balances - É o balanceamento de carga feito por software, a Microsoft dispões do Windows Network Load Balancing (NLB) faz parte do sistema operacional Windows Server e vem sendo aprimorado desde o Windows NT 4.0. No Windows 2008 R2 pode ser dimensionado para 32 hosts, mas é efetivo quando usado com até 8 hosts e sua maior vantagem é ser extremamente barato de implementar. Uma desvantagem é que não pode ser usado combinado com cluster do Windows, ou seja se for implementado uma solução com alta disponibilidade em que as funções de servidor Mailbox e Client Access estejam em dois servidores não poderá ser usado o NLB. Outra desvantagem é que ele suporta apenas afinidade IP de origem, ou nenhuma afinidade e isso limita a capacidade de efetivamente ter o equilíbrio entre todos os protocolos do servidor Client Access. O NLB também não tem inteligência embutida para testar a saúde do servidor ou funcionalidades antes de enviar o tráfego.

- Hardware Load Balancers - O balanceamento de carga de hardware é utilizado quando é necessário mais de oito nós em um site do Active Directory. Permite melhor desempenho e um número grande de recursos por ter um Hardware especializado. Suporta afinidades múltiplas e apoia a verificação de saúde do ambiente, que vão desde teste de ping simples para medir o tempo de resposta às páginas da Web personalizada. Com uma solução mais cara oferece redundância de hardware eliminando qualquer ponto de falha. Sua maior desvantagem é o custo de implantação, mas para implementação em grande escala é o mais recomendado.

- Application Firewalls - Aplicações firewall como o Microsoft Threat Management Gateway (TMG), ou o ForeFront Unified Access Gateway (UAG), são similares aos balanceadores de carga de hardware, mas podem fornecer recursos adicionais de segurança. Uma desvantagem é a sua complexidade, requer mais testes, mais suporte de administração e operação em relação as outras soluções. Outra desvantasgem é que não exercem equilíbrio de carga RPC e na necessidade dessa funcionalidade é necessário utilizar outra solução junto.

- DNS Round Robin - Usa a capacidade de mapear múltiplos hosts a um nome comum. Exemplo:

  mail.contoso.com 192.168.1.2

  mail.contoso.com 192.168.1.3

  mail.contoso.com 192.168.1.4

  O primeiro cliente a solicitar seria mail.contoso.com teria o endereço 192.168.1.2 retornado. o segundo teria 192.168.1.3, e ao terceiro 192.168.1.4. na quarta solicitação teria o primeiro endereço retornado novamente e assim subseqüentemente. Sua principal vantagem é a facilidade de construção. Seu ponto negativo é que não suporta afinidade o que requer que a aplicação mantenha a afinidade. Caso um servidor fique indisponível os navegadores Web continuam tentando chegar ao servidor indisponível por motivos de período de cache, que impossibilita o navegador de ser automaticamente direcionado para um servidor disponível nesse intervalo de tempo até que o cache expire. Outro problema é a falta de controle de limpeza ou remoção dos mortos, no exemplo dos três servidores caso um esteja com falhas e não esteja respondendo o servidor DNS continuará fornecendo o seu endereço a cada três consultas. E por ultimo as mudanças DNS são muito lentas ao se propagarem, no caso de um servidor novo ser adicionado ele ficará sendo subutilizado até o registro ser propagado plenamente. Por esses motivos o DNS round robin não é recomendado e sua utilização deve se limitar a ambientes de laboratório e implementações pequenas.

2.7.3 Alta Disponibilidade em Servidores de Transporte

Assim como nos servidores Client Access é necessário implantar vários servidores Hub Transport e Edge Transport para fornecer redundância no transporte de mensagens. É necessário implantar vários servidores Hub Transport em cada site do Active Directory fornecendo assim redundância e balanceamento de carga e a implantação de vários servidores Edge Transport fornecerão alta disponibilidade em serviços SMTP de entrada e saída.

Quando implantado vários servidores de transporte a redundância de sombreamento garante que as mensagens sejam protegidas contra perdas durante todo tempo que elas estão em trânsito. É atrasada a exclusão da mensagem do banco de dados dos servidores de transporte até que seja confirmada a entrega da mensagem com êxito em todos os saltos. Se verificado falha na entrega, o Exchange reenvia a mensagem para a entrega garantindo que a mensagem continue até chegar ao seu destino final.

Com a redundância de sombreamento e com vários servidores Hub Transport e Edge Transport se garante a alta disponibilidade sem perda de nenhuma mensagem em caso de falha em algum servidor de transporte e é possível remover um servidor para manutenção sem necessitar esvaziar as filas.

2.8 Boas Práticas em Servidores Edge Transporte

Como visto anteriormente a função de Servidor Edge Transport é designada para ser instalado em uma rede perímetro, exposto diretamente à Internet. Quando se coloca um servidor diretamente na Internet deve se ter maior cuidados em questões de segurança, no caso do servidor Edge Transport deve ser colocado em uma DMZ com um nível de segurança separando o servidor dos outros servidores Exchange da organização.

Ao utilizá-lo como servidor de borda para inspeção e segurança em e-mail deve ser levar em consideração alguns fatores que melhoram a segurança:

- Configuração clonada – É o processo em que se têm vários servidores com função de servidor Edge Transport com as mesmas configurações. É necessário clonar as configurações porque o Edge Transport não suporta o Windows Failover Clustering, que é a solução Microsoft que fornece alta disponibilidade em servidores de aplicação onde vários servidores estão ligados em um cluster.

- Status de notificação de entrega.

- Firewall de cabeçalho – É um mecanismo que remove campos de cabeçalho específicos de mensagens de entrada e saída. Os computadores

que executam a função de Hub Transport, ou Edge Transport instalado inserem campos de cabeçalho X personalizado no cabeçalho da mensagem. Um cabeçalho X é um campo de cabeçalho não oficial, definido pelo usuário, que existe no cabeçalho da mensagem. Ele não é especificado na RFC 2822, mas o usu de um campo de cabeçalho que comece por X- (no inglês, “X-readers”) tornou-se uma maneira aceitável de adicionar campos de cabeçalho não oficiais a uma mensagem.

Os campos de cabeçalho X contêm detalhes sobre as ações executadas nas mensagens pelos servidores de transporte. Essas informações podem configurar-se como possíveis riscos de segurança quando revelados a origens não autorizadas.

O Firewall de cabeçalho evita a falsificação desse cabeçalho, removendo-os das mensagens de entrada que entram na organização do Exchange vinda de fontes não confiáveis fora da organização do Exchange. Ele também impede a divulgação de cabeçalhos de roteamento padrão que são usados para rastrear o histórico de roteamento de uma mensagem.

2.9. Implantando Segurança com Firewall

2.9.1 Planejamento de Portas em Firewall

Como os servidores ficam na DMZ com acesso direto a Internet é necessário se configurar as portas que devem ser abertas no Firewall que separa o Edge Transport da Internet. Devem ser configuradas também as portas corretas no Firewall que o separa da rede interna e para melhorar a segurança deve ter o menor número de portas abertas, abaixo tabela com as portas necessárias para o transporte de mensagem da Internet.

Figura 20: Portas Requeridas no Firewall para o Edge Transsport

Direção de Firewall	Regra de Firewall	Descrição
External	Allow Port 25 - de todos endereços de IP externo para o Edge Transport	Habilita a entrada de mensagens SMTP vinda da Interner para o Servidor
External	Allow Port 25 - para todos endereços IP externo do servidor Edge Transport	Habilita o servidor Edge Transport para enviar mensagens SMTP para a Internet
External	Allow port 53 - para todos endereços IP externo de servidores Edge Transport	Habilita os servidores para resolver nomes da Internet Domain Name System (DNS)
Internal	Allow Port 25 - do servidor Edge Transport para especificados servidores Hub Transport	Habilita a transmissão de mensagens SMTP entrante para o Servidor Hub Transport na rede Interna
Internal	Allow Port 25 - dos especidivcados servidores Hub Transport para o servidor Edge Transport	Habilita a transmissão de mensagens SMTP saintes dos servidores Hub Transport para o servidor Edge Transport
Internal	Allow Port 50636 - (Secure Lightweight Diretory Access Protocol - LDAP) dos servidores Hub Transport que participam do EdgeSync com o servidor Edge Transport	Habilita o Hub Transport sincronizar o diretório de informação para o servidor Edge Transport usando o Edge Syncronization
Internal	Allow Port 3389 - Remote Desktop Protocol (RDP) da rede interna para o Edge Transport	Permite a adminstração remota do servidor Edge Transport

Fonte: Microsoft Exchange 2010 Best Practices (JAGOTT; STIDLEY, 2010, p. 298 e 299).

2.10 Prevenção de Desastres e Continuidade de Negócio

O Exchange Server 2010 apresenta uma plataforma de alta disponibilidade, que facilita a implantação de banco de dados de caixa de correio redundante e altamente disponíveis. Mas mesmo tendo uma plataforma que garante redundância extrema e maior grau de tolerância a falhas e desastres esses ainda podem ocorrer. Garantir que haja proteção suficiente para os dados essenciais é uma tarefa necessária. Para garantir maior recuperabilidade e menor tempo de parada é necessário se implantar uma rotina eficiente de Backup e Restauração, garantindo que se tenha um plano de continuidade de negócios em caso de falha ou desastre.

O Exchange 2010 suporta apenas backup baseados em VSS, sendo assim para fazer backup e restauração é necessário que a ferramenta com suporte ao Exchange que dê suporte ao gravador VSS para o Exchange 2010, como o Backup do Windows Server 2008, o Mycrosoft System Centes Data Protection Manager.

2.10.1 Recuperação do Servidor

Os servidores com funções de Mailbox, Client Access, Hub Transport, Unifid Messagin guardam a maioria das informações de configuração no Active Directory e em caso de falha em um servidor pode ser recuperado com um

parâmetro de instalação. Com o parâmetro de instalação /m:RecoverServer o servidor perdido é recompilado e recriado com as definições armazenadas no Active Directory.

A recuperação de um servidor perdido quase sempre se dá com a utilização de um novo hardware, mas pode também ser usado um servidor existente. Existem alguns requisitos para a restauração de um servidor perdido e a recuperação de um servidor perdido que faz parte de um grupo de disponibilidade deve ser diferente da forma como se recupera um servidor em outro modo operacional. Abaixo os requisitos necessários para recuperar um servidor que não faz parte de um DAG:

- O servidor que será realizado a recuperação deve ter o mesmo sistema operacional do servidor perdido.
- O novo servidor deve ter as mesmas características de desempenho do servidor perdido e a mesma configuração de hardware.
- O comando Setup /m:RecovereServer só é válido para servidores Hub Transport, Cliente Access, Mailbox e Unified Messaging o comando não se aplica a servidores Edge Transport.

O processo para recuperação de um servidor perdido está descrito abaixo:

1. Redefinir a conta de máquina do servidor danificado no Active Directory.
2. Instalar o sistema operacional do novo servidor é necessário colocar o mesmo nome do servidor danificado.
3. Ingressar o servidor ao mesmo domínio do servidor perdido.
4. Instalar os componentes do sistema operacional e os pré-requisitos do Exchange Server 2010.
5. Fazer logon no servidor com uma conta com direitos administrativos.

6. Com um prompt de comando deve se navegar até os arquivos de instalação do Exchange 2010 e executar o comando: Setup /m:RecovereServer.
7. Após terminar a instalação e antes de colocar o servidor em produção deve ser verificado possíveis customizações feitas anteriormente no servidor. Exemplo os temas do OWA que podem ser customizadas com o logo da empresa.

Para recuperar um servidor Mailbox que faz parte de um grupo de disponibilidade de banco de dados é necessário seguir as seguintes etapas:

1. Redefinir a conta de máquina do servidor danificado no Active Directory.DA
2. Instalar o sistema operacional do novo servidor é necessário colocar o mesmo nome do servidor danificado.
3. Ingressar o servidor ao mesmo domínio do servidor perdido.
4. Instalar os componentes do sistema operacional e os pré-requisitos do Exchange Server 2010.
5. Remover todas as cópias de banco de dados de caixa de correio que existem no servidor que está sendo recuperado.
6. Remover as configurações do servidor com falha do DAG.
7. Com um prompt de comando deve se navegar até os arquivos de instalação do Exchange 2010 e executar o comando: Setup /m:RecovereServer.
8. Após terminar deve ser adicionado o servidor ao DAG e adicionar as cópias de banco de dados.

O procedimento apresentado anteriormente é um meio extremo de recuperar um servidor Exchange 2010, deve ser empregado como ultima possibilidade quando o servidor não pode ser recuperado. O Windows 2008 e o Windows 2008 R2 incluem recursos de reparo de inicialização que podem recuperar um servidor em caso de arquivos corrompidos ou falta de arquivos. O processo de

reparo de inicialização também pode recuperar um servidor em caso de algum tipo de falha de boot envolvido com o gerenciador dor boot.

As ferramentas existentes no Windows 2008 e Windows 2008 R2 incluem:

- System Image Recovery.
- Windows Memory Diagnostics.
- Command Prompt.

Nos casos em que se tem falha em banco de dados e é necessário recuperar os dados do Exchange, também não há a necessidade de iniciar uma recuperação completa do servidor, em vez disso pode ser recuperado um banco de dados até o ponto de falha restaurando o backup completo mais recente.

O Servidor Edge Transport não guarda as informações do servidor no Active Directory, sua configurações são definidas por padrão, por serem atualizadas a partir da web, como nos dados antispam, ou por serem replicadas do Active Directory pelo processo de EdgeSync. Caso não tenha sido feito nenhuma customização o processo de recuperação é baseado na instalação de um novo servidor. Caso tenha sido feito customizações é necessário clonar para capturar todas as definições e usa-las em um novo servidor.

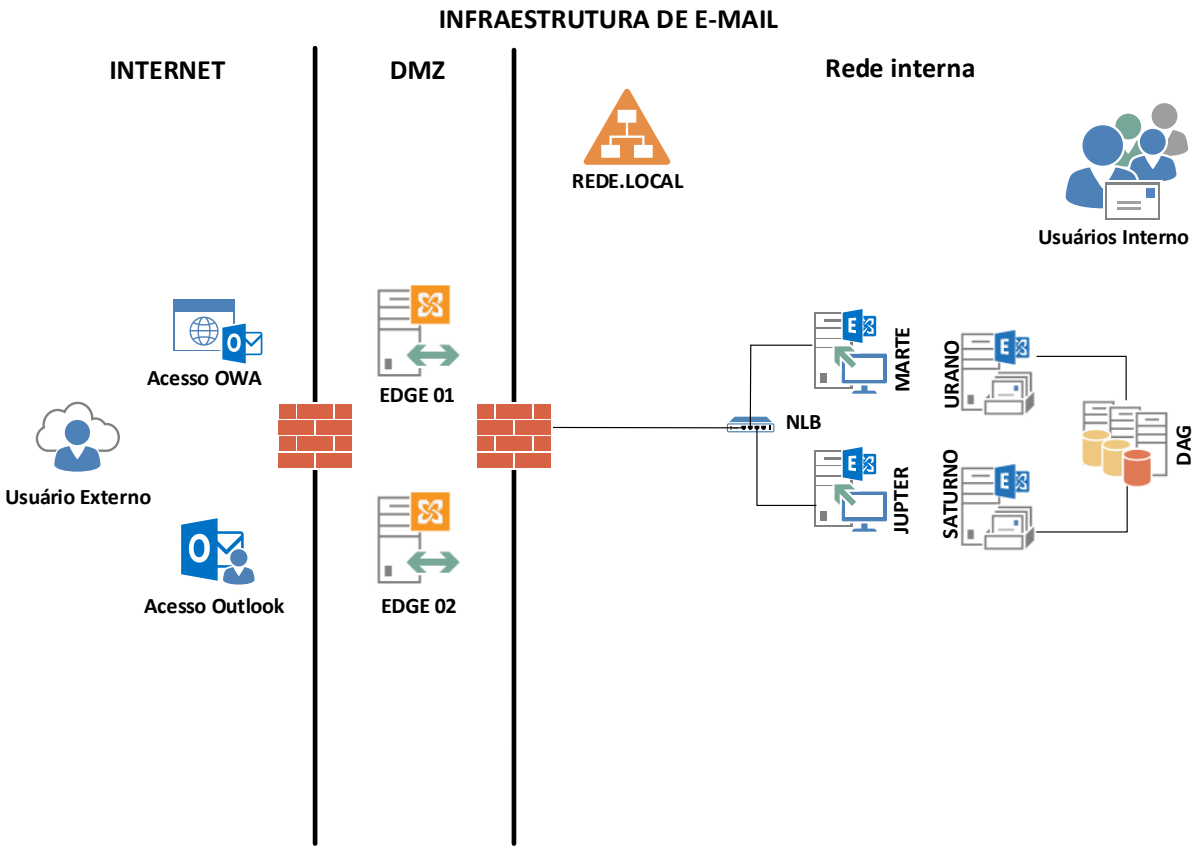
Existem dois scripts que automatiza todo processo de clone de servidor Edge Transport, o primeiro o ExportEdgeConfig.ps1 exporta todas as definições configurada pelo administrador e armazena em um arquivo.xml. O processo de restauração se baseia em copiar esse arquivo para o novo servidor e rodar o script ImportEdgeConfig.ps1, nesse processo o Exchange importará todas as definições configurada no arquivo.xml.

3. IMPLANTAÇÃO DA INFRAESTRUTURA SEGURA DE E-MAIL MICROSOFT

Visando ter disponibilidade, integridade e confidencialidade das informações em uma infraestrutura de e-mail, o trabalho contou com a instalação do MS Exchange Server 2010 em uma organização que utilizava uma ferramenta de e-mail “free” e dispunha do MS Windows 2008 com recursos do Active Directory. Após configurar a Solução Microsoft, foi habilitado caixa de correio em objetos de usuário do Active Directory e movido os dados da antiga solução.

O projeto buscou garantir a segurança dos e-mails armazenados nos servidores e em trânsito. Para alcançar os objetivos utilizou-se a infraestrutura abaixo:

Figura 22: Infraestrutura Implantada.



Fonte: elaborado pelo autor do trabalho.

Nessa perspectiva foi utilizados servidores em alta disponibilidade com Database Availability Group (DAG) nos servidores com função de Mailbox, CAS

Array nos servidores com função de Cliente Access, Network Load Balancing (NLB) em servidores com função de Hub Transport e servidores Edge Transport clonados. Tendo a criptografia como a base da segurança no transporte de e-mail, foi configurado o S/MIME, adquirido certificado digital para os usuários da organização, sugerido a utilização de Domain Security na comunicação entre organizações parceiras e integração do Exchange com uma infraestrutura de AD RMS. Será apresentado agora à execução da infraestrutura com suas configurações, não foi enfatizado migração de dados da antiga ferramenta de e-mail.

3.1 Criação de Organização Exchange

O processo de instalação do Microsoft Exchange Server 2010 cria a organização Exchange, antes de instalar o primeiro servidor foi necessário atender alguns pré-requisitos mínimos e de configurações para cada função de servidor. Abaixo relação de configurações necessárias:

- Nível funcional da floresta no mínimo Windows Server 2003 e o mestre de esquema deve executar no mínimo o Windows Server 2003 com Service Pack 1.

- Deve ser planejado o Active Directory.

- Instalar os pré-requisitos do sistema operacional básico para todas as funções de servidores: Microsoft .NET Framework 3.5 Service Pack, Gerenciamento Remoto do Windows (WinRM) 2.0 e o Windows PowerShell V2 (Windows6.0-KB968930.msu), em servidores que hospedarão a função de servidor Hub Transport ou Mailbox deve ser instalado o Microsoft Filter Pack.

Visando maior segurança deve ser instalado os componentes adicionais para cada função de servidor que será instalado.

3.1.1 Preparação do Active Directory

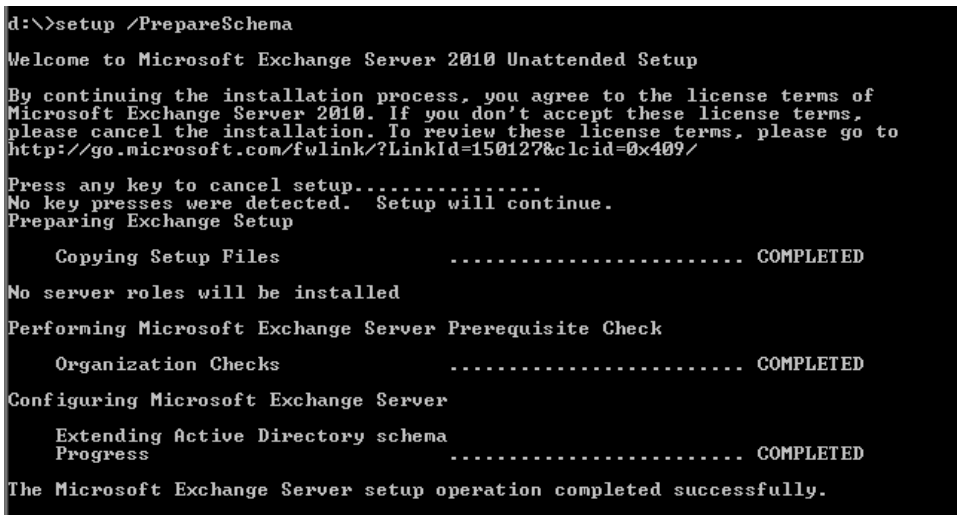
Ao instalar o Exchange Server 2010 se adiciona novos atributos ao esquema de serviço do domínio Active Directory e outras modificações em classes /atributos existentes. A organização já dispunha de uma infraestrutura do Active Directory e foi necessário apenas incrementar o esquema, as configurações e o domínio. Para fazer essas modificações é necessário procedimentos com alguns comandos e ao rodar os comandos foi monitorado o processo de replicação entre os controladores de domínio utilizado a ferramenta Active Directory Replication Monitor (replmon.exe). Após ser replicado entre todos os controladores de domínio é que se deu continuidade ao processo de preparação do Active Directory executando os comandos adicionais.

Quando se faz uma instalação limpa onde não existia uma organização do Exchange, nesse caso deve proceder da seguinte forma:

- Acessar o prompt de comando com direitos administrativos elevados e digitar o seguinte comando: setup /PrepareSchema ou setup /ps, e para executar esse comando deve ser usado uma conta que seja membro do grupo Administradores de Esquema e do Grupo Administradores de Empresa. Deve ser ainda executado em um computador 64 bits no mesmo domínio do Active Directory do controlador de esquema. Depois executar esse comando deve aguardar que as alterações sejam replicadas para toda a organização Exchange antes de continuar as próximas etapas. Esse comando faz várias modificações no esquema do Active Directory, todas as modificações podem ser encontradas em um documento da Microsoft disponível em:

  http://msdn.microsoft.com/en-us/library/dd877014(v=exchg.140.aspx.

Figura 21: Preparação do Esquema do Active Directory

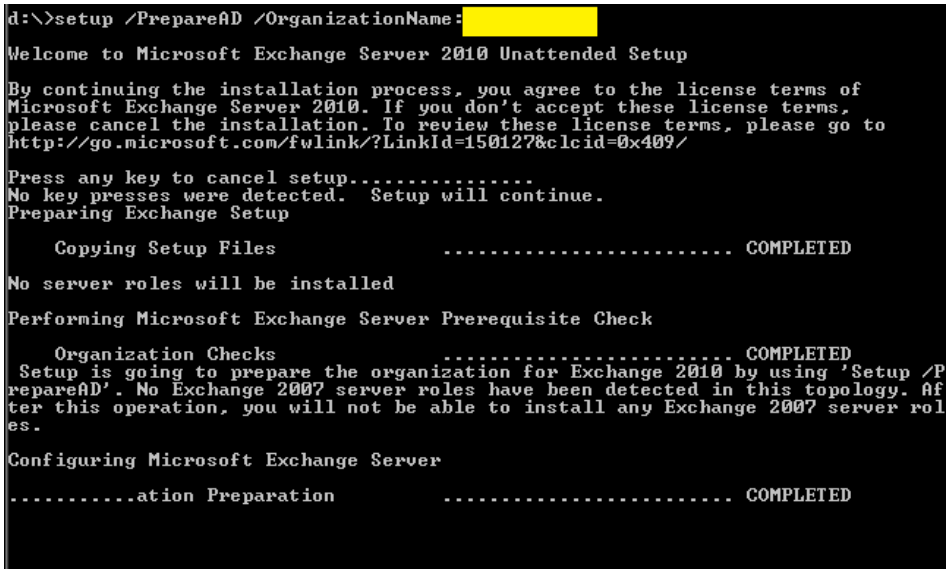


Fonte: elaborado pelo autor do trabalho

- Ainda no prompt de comando executar o comando: setup /PrepareAD [/OrganizationName: <nome da organização>] ou setup /p [/on:<nome da organização>]. Esse comando executa várias tarefas que criam a organização Exchange e os contêiner do Microsoft Exchange caso não exista. Esse comando também prepara o domínio local. Todas as tarefas executadas por esse comando está disponíveis em:

  http://technet.microsoft.com/en-us/library/bb125224.aspx

Figura 22: Preparação do Active Directory e Domínio Local.



Fonte: elaborado pelo autor do trabalho

3.1.2 Instalação de Funçóes de Hub Transport e Client Access

Como visto anteriormente um dos requisitos de segurança quando se pensa em uma infraestrutura de correio seguro com o Exchange Server 2010 se inicia na instalação dos servidores onde é instalado os componentes necessários para cada função. Para instalar os componentes necessários para a função de Servidor Hub Transport e Cliente Access são necessários os seguintes procedimentos:

- No Windows PowerShell executar o comando **ServerManagerCmd -i RSAT-ADDS**, este comando instala o programa LDIFDE no servidor.
- Após reinicializar o servidor no Windows PowerShell rodar o seguinte comando: **ServerManagerCmd -i Web-server Web-Metabase Web-Lgcy-Mgmt-Console Web-Basic-Auth Web-Windows-Auth Web-Net-Ext Web-Digest-Auth Web-Dyn-Compression NET-HTTP-Activation Web-ISAPI-Ext RPC-over-HTTP-proxy**.

Após esse preparatório o ambiente está preparado para receber o primeiro servidor Exchange 2010 da organização. Por questões de desempenho e escalabilidade é recomendado instalar os arquivos binários da instalação em um diretório diferente do de sistema. A forma de instalação foi customizada para se ter função de Hub Transport e Client Access no mesmo servidor. O mesmo procedimento foi feito em outro servidor e colocado em modo de alta disponibilidade para que em caso de falhas em um servidor o outro assuma as funções sem perda de mensagens ou quando for colocado um servidor off-line para manutenção não necessite de uma janela de manutenção.

Em ambientes grandes é recomendado colocar as funções de servidores Hub Transport, Client Access e Mailbox em cada site do Active Directory de forma que se tiver problemas em um link de WAN os serviços de e-mail continuem funcionando na localidade e quando for estabelecido a comunicação as mensagens destinadas a usuários que estão em outro site, ou fora da organização serão entregues. Caso não seja possível dispor dessa infraestrutura em todos os sites é recomendado colocar o modo de cache do outlook onde em caso de falhas de link aparecerá para o usuário como caixa offline, mas o usuário consegue acesso aos dados de e-mail armazenados em cache.

3.1.3 Instalação de Servidores com Função de Mailbox

Para instalar os componentes necessários para a função de Servidor Mailbox é necessário os seguintes procedimentos:

- No Windows PowerShell executar o comando **ServerManagerCmd -i RSAT-ADDS**, este comando instala o programa LDIFDE no servidor.
- Após reinicializar o servidor no Windows PowerShell rodar o seguinte comando: **ServerManagerCmd -i Web-server Web-Metabase Web-Lgcy-Mgmt-Console Web-Basic-Auth Web-Windows-Auth Web-Net-Ext Failover-Clustering**, esses comandos intala os componentes necessários para a instalação dos Servidores Mailbox que serão membros de um DAG.

Por questões de desempenho e escalabilidade é recomendado instalar os arquivos binários em diretório diferente do de sistema e colocar os banco de dados e os logs de transações em diretórios exclusivo com previsão de crescimento das base de dados. A forma de instalação é customizada para a função de Mailbox Server e foi modificado o local de instalação. O local padrão é: C:\Program Files\Microsoft\Exchange Server\V14

A organização foi configurada com serviço de alta disponibilidade aplicada nas bases de dados do Exchange, a alta disponibilidade é aplicada em caso de falha em um servidor, onde o outro assumirá todas as funções. Está sendo planejada a inclusão de alta disponibilidade em Data Centers, onde terá servidores em outra localidade para que em caso de falhas em no data center os serviços sejam providos por o outro data center.

3.1.4 Alta Disponibilidade nos Servidores de Transporte

Como visto anteriormente uma organização pode ser configurada apenas com servidores Hub Transport fazendo o roteamento de mensagens internas e externas, pode trabalhar com o conceito de Hub Transport para roteamento interno e Edge Transport para o roteamento externo, ou pode ter o Hub Transport para roteamento interno e um smart host para roteamento externo.

A organização em estudo compartilha as funções de CAS e HUB em dois servidores com alta disponibilidade, o processo de alta disponibilidade no HUB é

feita por meio do NLB, que será visto como foi criado adiante na implantação de alta disponibilidade do CAS. O Exchange cria automaticamente os conectores Send para o fluxo de mensagem interno, mas não cria os conectores Send necessários para o fluxo de mensagem para a Internet. Na organização foi criado os conectores send para a internet com o seguinte comando no Exchange Management Shell:

new-SendConnector -Name 'Internet Connector' -Usage 'Internet' -AddressSpaces 'SMTP:*;1' -IsScopedConnector $false -DNSRoutingEnabled $true -UseExternalDNSServersEnabled $false -SourceTransportServers 'SERVERHT1','SERVERHT2'

Com o comando foi criado o conector que envia as mensagens interna para a internet, mas a organização contará com o serviço de antispam na DMZ, será abordada posteriormente a implantação desse serviço e dos requisitos necessários antes de fazer a instalação do servidor.

3.1.5 Alta Disponibilidade nos Servidores Client Access

A organização em estudo tem dois servidores com função de Cliente Access, eles disponibilizam os acessos OWA, Active Sync, Autodiscover, POP3, IMAP4, RPC e Microsoft Outlook. Esses servidores estão configurados como Exchange CAS Array, o CAS Array não fornece redundância de falhas só, para total redundância foi combinado com o Cluster NLB do Windows Server 2008R2. Com essa configuração o serviço CAS Array agrupa os servidores e o Windows NLB balanceia a carga de trabalho.

3.1.5.1 Configuração do Windows NLB

Foi configurado o Netework Load Balancing (NLB) para balancear um conjunto de servidores CAS (Client Access Serevers). Alguns pontos a serem explicados:

- Foram utilizadas duas placas de rede para implantação do NLB.
- Utilizado configurações unicast para que funcione em todos os roteadores.

- Todos os nós estão na mesma subnet.
- Todos os servidores são baseados no Windows Server 2008 R2.
- Os servidores que fazem parte do Array não são membros de um DAG.
- O NLB foi instalado em todos os nós que fazem parte da estrutura.

Para instalação do NLB foi executado o seguinte comando no Windows Power Shell: ***ServerManagerCmd -i NLB***.

Após implantar o serviço NLB no Windows foi configurado os nós do NLB, procedimentos para essa configuração:

- Em Administrative tools selecionado Network Load Balancing Manager.
- Em Network Load Balancing Clusters com o botão direito do mouse clicar em New Cluster, digitar o nome do servidor em Host e mandar conectar. Selecionar a interface que será usada pelo NLB.
- Em cluster IP Address foi adicionado o IP que será compartilhado por todas as máquinas do NLB e nos quais os clientes utilizarão como referência, esse IP é conhecido como VIP (Virtual IP).
- Em Cluster Parameters foi especificado o nome de uso do NLB e o modo de operação unicast.
- Em Port Rules foram adicionado os protocolos que serão utilizados pelos serviços do CAS: TCP 59595, TCP 443, TCP 80, TCP 110, TCP 995, TCP 143, TCP 993, TCP 135, TCP 25 e UDP 500.

Após ser criado o cluster foi adicionado outro servidor ao cluster NLB. E foi criada a entrada para na Zona DNS utilizando o VIP que é o IP definido durante a criação do Cluster, e feito teste de funcionamento baseado nos protocolos criados na regra. Para concluir os serviços de alta disponibilidade foi configurado o Client Access Array, foi executado o seguinte comando no Exchange Management Shell (EMS): ***New-ClientAccessArray -Fqdn "Nomedocluster" -Site "NomedoSite"***. E por fim foi adicionado os banco de dados de caixa de uma só vez a matriz CAS com

o comando no EMS: ***Get-MailboxDatabase | Set-MailboxDatabase -RpcClientAccessServer "NomedoCluster"***. Com esses procedimentos está configurada a alta disponibilidade para acesso de clientes MAPI usando o Client Access Array. Os serviços de alta disponibilidade para os outros clientes estão sendo ofertado pelo NLB e foi configurado para utilização interna da seguinte maneira:

- Configuração OAB: Usando o EMS para verificação o valor atual utilizado ***Get-OabVirtualDirectory | select Server,InternalURL***, e substituido o nome do servidor local pelo nome que foi dado ao serviço ao gerar o certificado ***Get-MailboxDatabase |Set-MailboxDatabase -RpcClientAccessServer "https://Fqdn NLB "***.

- EWS: ***Get-WebServicesVirtualDirectory | Set-WebServicesVirtualDirectory -InternalUrl https://webmail.domínio/EWS/Exchange.asmx***.

- Autodiscover: ***Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalURL https://webmail.dominio/autodiscover/autodiscover.xml***. Por padrão o altodiscover não é habilitado e já havia sido habilitado e configurado para acesso interno sem segurança e foi configurado para acesso com SSL.

- ActiveSync: ***Get-ActiveSyncVirtualDirectory | Set-ActiveSyncVirtualDirectory -InternalUrr Https://webmail.dominio/Microsoft-Server-ActiveSync***.

- OWA: ***Get-OwaVirtualDirectory | Set-OwzVirtualDirectory -InternalURL https://webmail.dominio/owa***.

- ECP: ***Get-EcpVirtualDirectory | Set-EcpVirtualDirectory -InternalURL https://webmail.domínio/ecp***.

Com esse procedimento foi concluído o processo de criação de dois servidores com função de CAS e HUB de forma que se tem coexistência e alta disponibilidade das funções.

3.1.6 Alta Disponibilidade em Servidores Mailbox

3.1.6.1 Planejamento de Rede na Implantação do DAG

Os servidores que fazem parte do DAG foi desabilitado alguns componentes do IPv6, foi procedido da seguinte forma:

1. Editado o registro do Windows nos dois servidores por meio do Regedit.

2. Cave: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters***, foi criado a entrada ***DisabledComponents*** da seguinte forma:

    - Em editar, novo e em Valor DWORD (32 bits), digitado ***DisabledComponents***.

    - Após ser criado o ***DisabledComponents*** foi editado com os valores ***0xffffffff*****,** esse valor desabilita todos os componentes do IPv6, exceto a interface de loopback do IPv6.

Para o perfeito funcionamento da rede de replicação e de acesso a clientes é importante ter um mínimo de duas placas de redes em cada servidor membro do DAG, a configuração de rede é algo bem simples, mas caso não seja configurado corretamente pode se ter problemas na hora de implementar o DAG. E alguns pontos são importantes no aspecto de rede:

- Todos os membros de um mesmo DAG deve ter o mesmo número de interface.

- Pode ser usada mais de uma rede de replicação e pode ser utilizado também Teaming de adaptadores nessa rede.

- Independente da distância entre os membros do DAG não é suportado uma latência superior a 250ms entre os membros.

- Protocolo APIPA não é suportado.

Na instalação do DAG houve uma falha, que após algumas hora foi resolvido verificando a ordem das interfaces, estavam com ordens trocadas nos servidores. Outro ponto é a remoção dos componentes ***Client for Microsoft Networks*** e ***File and Printers Sharing for Microsoft Networks***. Não deve ser configurado Geteway nem DNS nas interfaces relacionadas a replicação e deve ser desmarcado a opção ***Register this connection's address in DNS***.

Para melhor visualização foi renomeado as interfaces de rede dos servidores da seguinte forma:

- MAPI - Rede onde é feito acesso dos clientes e outros servidores ao DAG.
- Replication - Rede onde ocorre a replicação das base de dados.

As configurações estão da seguinte forma:

3.1.6.2 Alta Disponibilidade de Banco de Dados

Antes de implantar o DAG é necessário criar o objeto de rede de cluster (CNO) e atribuir as devidas permissões ao mesmo. Os passos a seguir foram feitos na organização:

- Criado uma conta de computador para o CNO, a conta foi criada na mesma OU onde estão os objetos dos servidores Exchange.
- A conta de computador do CNO foi adicionada ao USG do Subsistema Confiável do Exchange, isso foi feito colocando a conta ao grupo ***Exchange Trusted Subsystem***.

Para criar o Grupo de Disponibilidade de Banco de dados, foi usado o seguinte comando no Exchange Management Shell:

New-DatabaseAvailabilityGroup -Name DAG1 -
DatabaseAvailabilityGroupIpAddresses 10.0.0.100

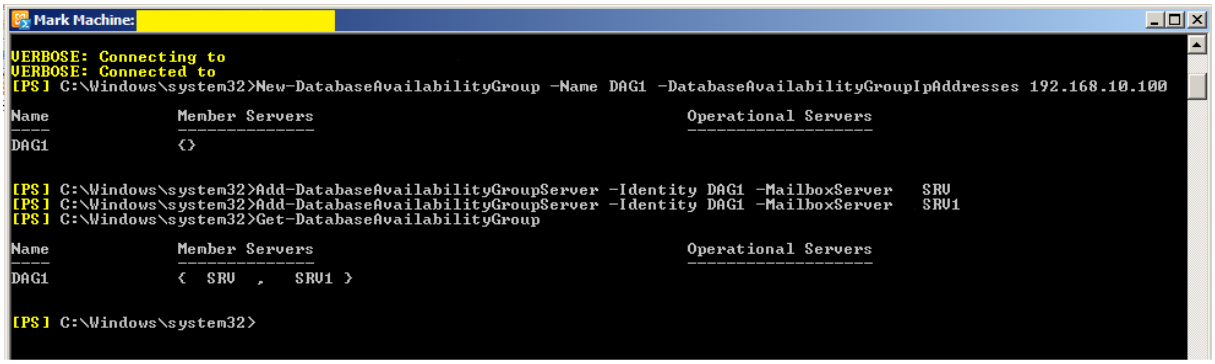
Esse comando cria o grupo de disponibilidade de banco de dados e a rede de replicação de dados. Para adicionar os servidores membros do grupo de disponibilidade foi usado os comandos abaixo:

Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer "MailBox1"

Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer "MailBox2"

Na organização implantada o procedimento instalou com sucesso os recursos de alta disponibilidade de base de dados do Exchange 2010, na figura abaixo pode se ver que foi criado o DAG e os dois servidores estão como membro do dag. Em caso de falha, deve ser verificado em C:\ExchangeSetupLogs\DagTasks e verificado o arquivo correspondente ao erro, após verificar o erro deve fazer os procedimentos de troubleshooting.

Figura 23: Verificação de Membros de DAG.



Fonte: elaborado pelo autor do trabalho.

Os procedimentos criaram a rede de replicação e o failover cluster. A rede pode ser verificada no Exchange Management Console em Organization Configuration, Mailbox e clicando em Database Availability Groups.

Foram criadas as bases de dados no servidor principal segundo as políticas de cotas para cada setor, depois adicionado cada banco de dados ao grupo de disponibilidade. Segue exemplo de como criar e colocar uma base de dados em alta disponibilidade. Comando para criar a base de dados para os usuários da CGTI:

new-mailboxdatabase -Server 'ServerName' -Name 'CGTI' -EdbFilePath 'E:\Program Files\Microsoft\Exchange Server\V14\Mailbox\CGTI\CGTI.edb' -LogFolderPath 'E:\Program Files\Microsoft\Exchange Server\V14\Mailbox\CGTI'

- Comando para montar a base de dados:

mount-database -Identity 'CGTI'

- Colocar o banco de dados em alta disponibilidade:

Add-MailboxDatabaseCopy -Identity 'CGTI' -MailboxServer 'MailBoxServer2' -ActivationPreference '2'

A organização tratada nesse projeto de conclusão de curso tem 50 base de dados em alta disponibilidade e foi utilizado um script que fez a leitura de um arquivo .csv e criou as base de dados e outro script que colocou as base de dados em alta disponibilidade.

3.2 Segurança no Acesso de Clientes de E-mail

O acesso disponibilizado por servidores com função de Client Access na organização e que fazem parte do Cluster e Array são todos seguros e a segurança é baseada no conceito de SSL. Para alcançar os objetivos de segurança foi solicitado um certificado válido por uma autoridade certificadora subordinada à hierarquia do ICP-Brasil. O ideal seria certificados para alguns serviços, mas como não foi possível, foi gerado um certificado curinga (*.domínio), e exportado e importado nos servidores que fazem parte do relay. Após ser importado o certificado foi atribuído ao IIS, POP3 e IMAP4. Processo utilizado com o EMS: ***Enable-ExchangeCertificate -thumbprint <certificado> -Services "IIS,POP,IMAP"***. Para finalizar as configurações foram utilizados os seguintes passos:

- Segurança no Exchange Active Sync: Foi configurado os diretórios virtuais do Microsoft Excahnge ActiveSync para usar o protocolo SSL. No gerenciador IIS, em site padrão, em propriedades do diretório virtual Microsoft-Server-ActiveSync, na guia Comunicações Seguras foi editado para requerer canal seguro.

- Canal seguro no Outlook Anywhere: No diretório virtual rpc foi editado para requerer canal seguro.

- Segurança no POP3 e IMAP4: São usados os protocolos TLS e SSL para proteger conexões entre os usuários e os servidores Exchange Server da organização. Foi configurado o serviço POP3 para usar segurança TLS ou SSL no EMS: ***Set-PopSettings -Server "Nome do Servidor" -X509CertificateName "Nome do Certificado"***. E no IMAP: ***Set-ImapSettings -Server "Nome do Servidor" -X509CertificateName "Nome do Certificado"***. Depois foi usado o Shell para configurar a autenticação no POP3 e no IMAP4: ***Set-PopSettings -LoginType SecureLogin*** e ***Set-ImapSettings -LoginType SecureLogin***. E para finalizar foi configurado as portas não sendo as padrões utilizada para comunicação do POP3 e IMAP4: ***Set-PopSettings -SSLBindigs IPaddress:Port*** e ***Set-ImapSettings -SSLBindings IPaddress:Port***.

- Foi configurado os diretórios virtuais do Outlook Web App para usarem SSL da seguinte forma: No gerenciador do IIS, no site padrão onde está hospedado os diretórios virtuais do Outlook Web App em configurações do SSL foi selecionado para exigir SSL de 128 bits. Em certificado de clientes ficou selecionado ignorar. Foi habilitado ainda o funcionamento de S/MIME no EMS: ***Set-OWAVirtualDirectory -identity "owa(Defout Web Site)" -SMimeEnabled $true***.

O Acesso Externo aos serviços ofertados pelos Servidores Client Access são protegidos por Firewall que libera acesso apenas as portas configuradas para cada serviço e que comunicam diretamente com servidores proxy reverso no TMG que remetem as solicitações ao CAS-NLB. Antes de serem publicados os serviços foram configuradas as propriedades de URL Externa no EMS:

- Diretório virtual Exchange Active Sync: ***Set-ActivesyncVirtualDirectory -Identity "CAS_Server_Name\Microsoft-Server-ActiveSync (Default Web Site)" -ExternalURL Https://mail.dominio/Microsoft-Server-Activesync***

- Diretório Virtual do Outlook Web App: ***Set-OwaVirtualDirectory -Identity "CAS_Server_Name\Owa (Defaut Web Sit)" -ExternalURL Https://mail.dominio/OWA***

- Diretório Virtual de Serviços Web do Exchange: ***Set-WebServicesVirtualDirectory -Identity "CAS_Server_Name\EWS (Default Web Site)" -ExternalUrl https://mail.domínio/ews/exchange.asmx***

- Diretório Virtual Outlook Anywhere: ***Enable-OutlookAnywhere -Server NOME_NLB -ExternalHostname "mail.Domínio"***

3.3 Auditoria da Organização Exchange

Requisitos legais são necessários em todas as organizações, visando transparência na administração do ambiente de e-mail e como medida de auditar a administração do sistema de correio eletrônico foi modificado o log de auditoria que por padrão é configurado para três meses. Utilizado o comando no EMS: ***Set-AdminAuditLogConfig -AdminAuditLogAgeLimit 1825.00:00:00***. Como requisito da coordenação se faz necessário um relatório mensal de auditoria e foi gerado um scrip e agendado a tarefa que gera o relatório mensal e coloca em um diretório no servidor. O administrador coleta essa informação e transfere para o diretório de rede onde estão armazenados os relatórios gerenciais.

Com essa configuração se é auditado os Cmdlets que são executados diretamente no Shell de gerenciamento do Exchange

3.4 Auditoria dos Servidores Exchange

A auditoria está configurada para permitir o controle do que está acontecendo com o Exchange Server. É possível usar a auditoria para coletar informações relacionadas à logons e logoffs, uso de permissões e muito mais e quando ocorre uma ação que foi configurada para a auditoria a ação fica gravada no log de segurança do sistema. Por padrão a Microsoft guarda as informações de log em arquivos que ao atingir o tamanho configurado é reescrito. Para atender os requisitos legais a organização em estudo tem implantado um servidor de log para armazenar os dados por um período maior. Abaixo dados de auditoria que foi habilitado na organização por meio de uma GPO que coleta os seguintes eventos:

- Audit Account Logon Events: Controla a autenticação das contas de usuários durante o logon.

- Audit Account Management: Controla o gerenciamento de conta por meio do usuário e computadores do Active Directory. Eventos são gerados quando um usuário acessa o diretório.

- Audit Object Access: Controla o uso de recursos do sistema para caixa de correio, information store e outros tipos de objetos.

- Audit police Change: Controla as alterações feitas aos diretórios de usuário, auditoria e relação de confiança.

- Audit Privilege Use: Controla o uso de direitos e privilégios do usuário como o direito de criar caixas de correio.

- Audit System Events: Controla a inicialização, desligamento e reinicialização do sistema, além das ações que afetam a segurança ou o log de segurança.

3.4 Higienização de Mensagens

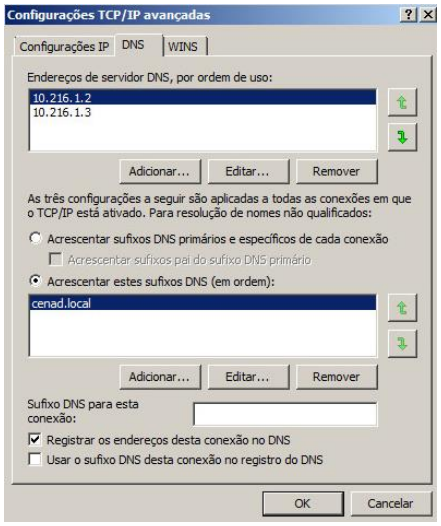
3.4.1 Edge Transport

A limpeza dos e-mails vindos da Internet é feita na DMZ antes de entrar na organização Exchange. Esse serviço é ofertado pela função Edge Transport e antes de instalá-lo se atendeu alguns pré-requisitos e também foi planejado o local dos servidores na rede. Basicamente o Edge é a única regra que pode estar em uma DMZ, ele não deve estar no domínio. Em alguns cenários de clientes onde vários servidores Edge são necessários (falando aqui em uma implantação com mais de 10 servidores Edge) o uso de um AD na DMZ para controlar as configurações do Edge pode se fazer necessário, mas no caso da organização estudada que tem apenas dois servidores com configuração clonada não é necessário a inclusão de um AD na DMZ.

Antes de instalar a função são necessárias Algumas configurações, abaixo procedimento executado na Infraestrutura antes de instalar os servidores com função de Edge Transport.

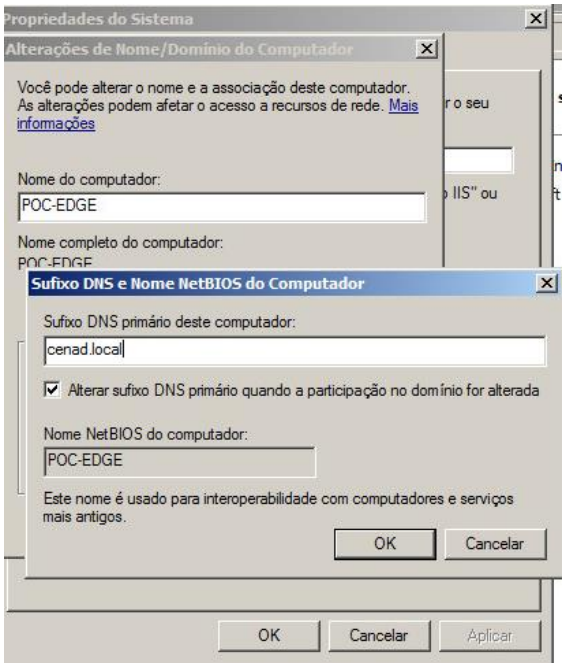
- Configuração de sufixo DNS do servidor, colocando as informações referentes ao domínio:

Figura 24: Adicionar Sufixo DNS em Configurações de Interface de Rede.



Fonte: elaborado pelo autor do trabalho

Figura 25: Adicionar Sufixo DNS para o Computador.



Fonte: elaborado pelo autor do trabalho

- Criação de registro no DNS Interno para que os Servidores Hub Transporte possa resolver o nome dos servidores Edge Transport.

- Instalar pré-requisitos de funções no Windows 2008R2:

  ServerManagerCmd.exe –i net-framework-core telnet-client adlds

- Instalação de função Edge Transport no servidor com a mídia de instalação do Exchange 2010.

Após instalar a função no servidor foi necessário configurar a sincronização com toda a estrutura de e-mail da organização Exchange. Esse processo se deu com as configurações de Edge Subscription. O Arquivo subscription faz com que o serviço de envio e recebimento funcione corretamente. O mesmo é responsável em fazer o sincronismo do servidor EDGE com o restante da organização Exchange Server 2010. O Arquivo é gerado com o comando no Shell do Exchange:

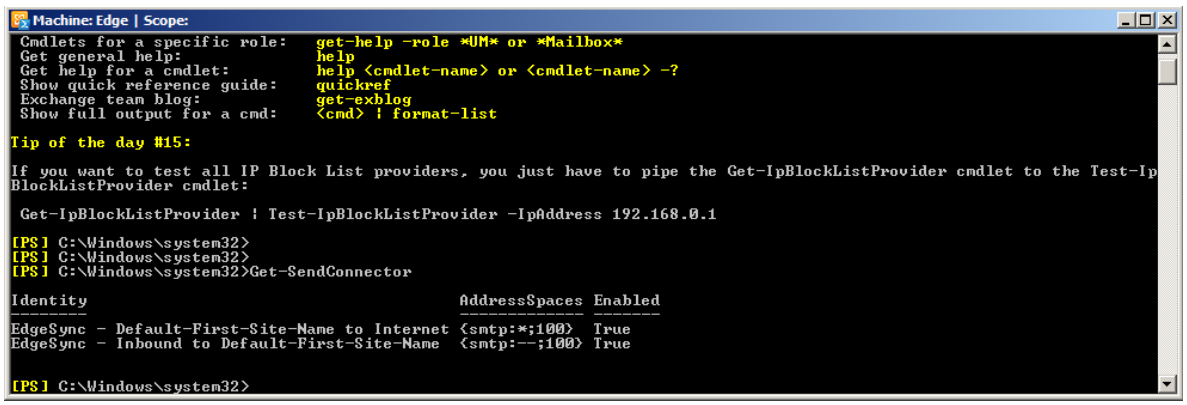
New-EdgeSubscription –filename c:\arquivo.xml –Site "Default-First-Site-Name"

Levado o arquivo para o servidor Hub Transport e feito configurações de nova assinatura de borda, após esse procedimento foi sincronizado os dados com o servidor Edge com os comandos:

Start-EdgeSynchronization

Durante a inscrição foi especificado o site do Active Directory associado na inscrição, com isso os servidores Hub Transport no site executam o serviço de EdgeSync e são responsáveis por sincronizar os dados de configuração entre o Active Directory Domain Service e o AD LDS no servidor Edge. Por padrão o serviço de EdgeSync sincroniza os dados de configuração a cada hora e os dados de destinatários a cada quatro horas. Com esses procedimentos deve ser criado um conector send para enviar mensagens para a Internet e um conector inbound, isso pode ser visualizado com o comando no shell do Exchange: ***Get-Sendconnector***. E a saída deve ser parecida com a saída abaixo:

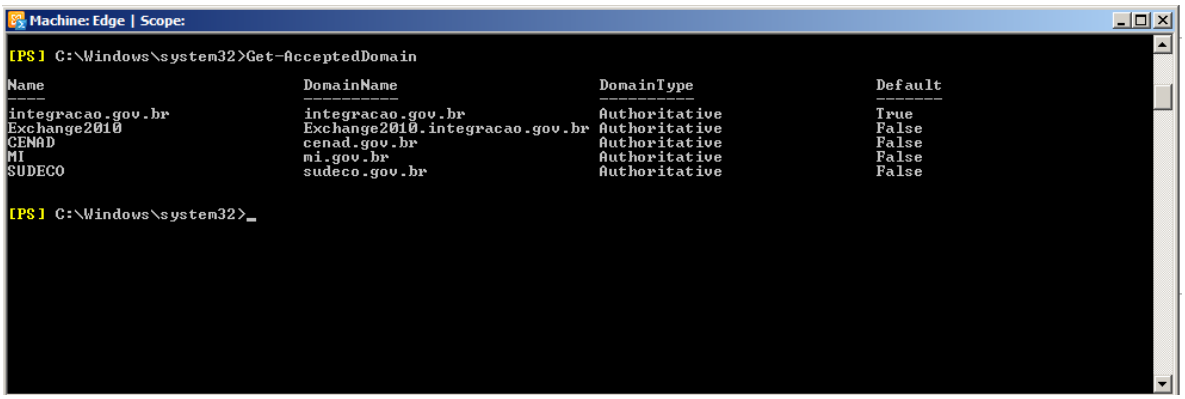
Figura 26: Verificação de Conectores de Envio.



Fonte: elaborado pelo autor do trabalho

E devem ser criadas as entradas para os domínios aceitos, que pode ser verificado com o comando ***Get-Acceptddomain***.

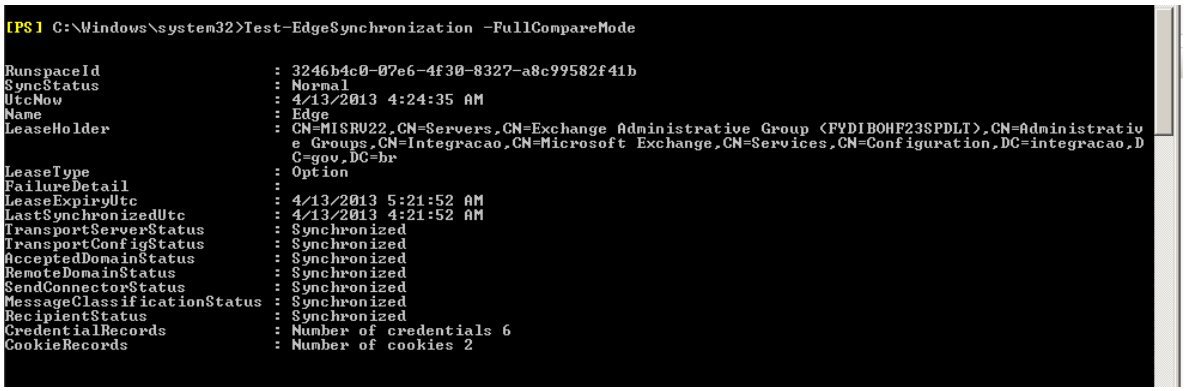
Figura 27: Verificação de Domínios Aceitos.



Fonte: elaborado pelo autor do trabalho

E por ultimo deve ser verificado se a inscrição ocorreu com sucesso e se todos os dados necessários foram replicados, isso pode ser verificado com o comando shell do Exchange: ***Test-EdgeSynchronization -FullCompareMode –Confirm.*** A saída do comando deve ser semelhante a seguinte tela:

Figura 28: Verificação Replicação do Hub Transport para Edge Transport.



Fonte: elaborado pelo autor do trabalho

A parte de instalação e sincronização do servidor Edge Transport está finalizada, faltando apenas as configurações adicionais nos filtros de Spam e inclusão de um IP Block List Provider, no caso da organização em estudo foi inscrito no Spamhouse.org, (http://www.spamhaus.org/zen/), para inscrição nesse provedor foi feito pelo comando no Shell do Exchange:

Add-IPBlockListProvider -Name "Spam haus" -LookupDomain zen.spamhaus.org -AnyMatch $true

Para refinar as configurações de spam ou outros e-mails indesejados foi aberto canal com os usuários do serviço de e-mail da organização informando as modificações feitas na infraestrutura de e-mail e que no caso de recebimento de spam deve ser enviado para o e-mail, higienização.email@integracao.gov.br para que seja tratado pelos administradores do serviço de e-mail. Os filtros de spam foram configurados e criado uma caixa de correio de quarentena onde os e-mail que caírem em quarentena serão armazenados, (quarentena@integracao.gov.br), a caixa de quarentena deve ser verificada diariamente e tratado possíveis falso/positivo de spam. Os filtros habilitados e configurados para tratamento de mensagens entrantes estão abaixo:

- Filtragem de conteúdo.
- Filtragem por destinatário.
- Filtragem por remetente.
- ID de remetente.

- Lista de IP bloqueados.
- Lista de IPs permitidos.
- Provedor de lista de bloqueio de IP.
- Reputação do remetente.

3.5 Regras em Firewall

A organização conta com Firewall Check Point e com o TMG para fazer a segurança da infraestrutura de e-mail e publicação dos serviços do Exchange 2010. Abaixo as portas abertas e serviços utilizados por função de servidores.

Figura 29: Portas Abertas em Firewall Check Pointe para comunicação dos Servidores de Transport (Edge Transport Server e Hub Transport Server - Configurações feitas em rede de servidores, Rede DMZ e Rede Local).

Configurações Para Servidores de Transport (Edge Transport e Hub Transport)					
Caminho	Portas	Autenticação Padrão	Autenticação Aceita	Criptografia	Criptografado
Hub Transport para Hubtransport	25/TCP (SMTP)	Kerberos	Kerberos	Sim Usando TLS	Sim
Hub Transport para Edge Transport na DMZ	25/TCP (SMTP)	Confiança Direta	Confiança Direta	Sim Usando TLS	Sim
Edge Transport na DMZ para Hub Transport	25/TCP (SMTP)	Confiança Direta	Confiança Direta	Sim Usando TLS	Sim
Edge Transport na DMZ para Edge Transport na DMZ	25/TCP (SMTP)	Anônimo, Certificado	Anônimo, Certific	Sim Usando TLS	Sim
Mailbox Server para Hub Transport	135/TCP (RPC)	NTLM/Kerberos	NTLM/Kerberos	Sim, Usando Criptografia RPC	Sim
Hub Transport para Mail Box Server	135/TCP (RPC)	NTLM/Kerberos	NTLM/Kerberos	Sim, Usando Criptografia RPC	Sim
Hub Transport para Edge Transport na DMZ	50636/TCP (SSL)	Básica	Basica	Sim, Usando LDAP sobre SSL (LDAPS)	Sim
Hub Transport para Active Directory	389/TCP/UDP (LDAP), 3268/TCP (LDAP GC), 88/TCP/UDP (Kerberos), 53/TCP/UDP (DNS), 135/TCP (RPC netlogon)	Kerberos	Kerberos	Sim, Usando Criptografia Kerberos	Sim
Clientes SMTP para Hub Transport	587 (SMTP) 25/TCP (SMTP)	NTLM/Kerberos	NTLM/Kerberos	Sim , Usando TLS	Sim

Fonte: elaborado pelo autor do trabalho

Figura 30: Portas Abertas em Firewall Check Pointe para comunicação dos Serviços de Servidores com Função de Mailbox (Mailbox para Servidores Client Access e AD – Rede de Servidores).

Configurações Para Servidores com Função de Mailbox					
Caminho	Portas	Autenticação Padrão	Autenticação Aceita	Criptografia	Criptografado
Mailbox Server para Active Directory	389/TCP/UDP (LDAP), 3268/TCP (LDAP GC), 88/TCP/UDP (Kerberos), 53/TCP/UDP (DNS), 135/TCP (RPC netlogon)	Kerberos	Kerberos	Sim, Usando Criptografia Kerberos	Sim
Acesso Remoto (Registro Remoto)	135/TCP (RPC)	NTLM/Kerberos	NTLM/Kerberos	Sim Usando IPSEC	Não configurada
Acesso Remoto (SMB/Arquivo)	445/TCP (SMB)	NTLM/Kerberos	NTLM/Kerberos	Sim Usando IPSEC	Não configurada
Serviços Web Cliente Access Server	135/TCP (RPC)	NTLM/Kerberos	NTLM/Kerberos	Sim Usando IPSEC	Sim
Mailbox Server para Mailbox Server Serviço de Clustering	135/TCP (RPC)	NTLM/Kerberos	NTLM/Kerberos	Sim, Usando Ipsec	Não configurada
Indexação de Conteúdo	135/TCP (RPC)	NTLM/Kerberos	NTLM/Kerberos	Sim, Usando Criptografia RPC	Sim
Serviços de Topologia do Active Directory do Microsoft Excahnge - Caminho DC	135/TCP (RPC)	NTLM/Kerberos	NTLM/Kerberos	Sim, Usando Criptografia RPC	Sim

Fonte: elaborado pelo autor do trabalho

Figura 31: Portas Abertas em Firewall Check Pointe para comunicação dos Serviços de Servidores com Função de Client Access (Client Access para rede de servidores, Client Access para Rede Local, Client Access para DMZ – Na DMZ está o TMG que publica serviços de Active Sync, OWA, HTTPs over RPC e todos os Serviços disponíveis para os clientes de e-mail).

Configurações Para Servidores com Função de Mailbox					
Caminho	Portas	Autenticação Padrão	Autenticação Aceita	Criptografia	Criptografado
Acesso ao Active Directory	389/TCP/UDP (LDAP), 3268/TCP (LDAP GC), 88/TCP/UDP (Kerberos), 53/TCP/UDP (DNS), 135/TCP (RPC netlogon)	Kerberos	Kerberos	Sim, Usando Criptografia Kerberc	Sim
Descoberta Automática - Clientes	80/TCP, 443/TCP (SSL)	Windows Integrada/Básica (Negociar)	Básica, Resum	Sim, usando HTTPS	Sim
Serviço de Disponibilidade	80/TCP, 443/TCP (SSL)	NTLM/Kerberos	NTLM/Kerberos	Sim, usando HTTPS	Sim
Replicação de Caixa de Correio	808/TCP	NTLM/Kerberos	NTLM/Kerberos	Sim, usando HTTPS	Sim
POP3	110/TCP (TLS), 995/TCP (SSL)	Basica/Kerberos	Basica/Kerberc	Sim, usando SSL, TLS	Sim
IMAP	143/TCP (TLS), 995/TCP (SSL)	Basica/Kerberos	Basica/Kerberc	Sim, usando SSL, TLS	Sim
OWA	80/TCP, 443/TCP (SSL)	Autenticação Baseada em Formulários	Autenticação Básica, Resumida, Baseada em Formulários, NTLM (somente v2), Kerberos,	Sim, Usando HTTPS	Sim, Usando Certificado.
Outlook Anyw are	80/TCP, 443/TCP (SSL)	Básica	Básica ou NTLM	Sim, Usando HTTPS	Sim
Active Sync	80/TCP, 443/TCP (SSL)	Basica	Basica, Certificado	Sim, Usando HTTPS	Sim
Client Access para Mailbox Server	RPC	Kerberos	NTLM/Kerberos	Sim, Usando Criptografia RPC	Sim
Client Access para Client Access	80/TCP, 443/TCP (HTTPS)	Kerberos	Kerberos	Sim, usando SSL	Sim

Fonte: elaborado pelo autor do trabalho

3.6 Configurações em DNS

No DNS interno foi configurado registro para que possa ser resolvido nome dos servidores Edge Transport. No DNS Externo foi criado registro MX com mesmo peso para que seja feito redundância de e-mail entrantes vindo da Internet. Foi feito configurações de registro SPF para validar e-mails enviados do domínio.

CONCLUSÃO

O estudo permitiu compreender que o correio eletrônico, como pensado no início, não garante as bases da segurança da informação: integridade, confidencialidade, disponibilidade, autenticidade e não repudio. Que existe a necessidade de mecanismos adicionais para proteger as mensagens em transporte, evitar o recebimento de mensagens indevidas, proteger as mensagens armazenadas em servidores de e-mail ou na máquina do usuário, garantir a disponibilidade dos dados e que os mesmos estejam íntegros e acessíveis apenas a quem é de direito. Permitiu ainda compreender que usando as boas práticas de segurança na configuração de um servidor de e-mail se pode minimiza as principais ameaças existentes.

O Estudo apresentou o MS Exchange Server 2010 como uma ferramenta de correio eletrônica robusta que permite ao administrador implantar uma organização de forma a garantir as bases da segurança da informação. Podem ser utilizados mecanismos criptográficos para tratar problemas de captura de mensagens em trânsito, inviabilizando a leitura da informação capturada e que podem dar subsídios para futuras fraudes. A assinatura digital para garantir a autenticidade e não repúdio da informação. Servidores com função de Edge Transport fazendo o tratamento de spam, reduzindo o número de e-mails fraudulentos recebidos e possibilitando a remoção de vírus que são causas constantes de fraudes. O trabalho apresentou técnicas que garantem a disponibilidade dos dados de e-mail em caso de falha em um servidor e até em um datacenter e algumas ferramentas de segurança que integram a solução.

O Estudo propôs a criação de uma infraestrutura segura com alta disponibilidade. A solução consiste no mínimo de sete servidores onde se é implantado quatro funções de servidores, o Mailbox Server com DAG para as bases de dados em alta disponibilidade, o Hub Transport Server e Client Access Server compartilhando os mesmos Hardwares em cluster com Array e o Edge Transport Server em uma DMZ fazendo a analise de conteúdo e trabalhando integrado com o ForeFronte Protection For Exchange 2010 para analise de conteúdo e Higienização de mensageria. O estudo propõe ainda a utilização de técnicas criptográficas para comunicação entre os servidores de transporte, a utilização de S/MIME para os

clientes de e-mail enviar e-mails criptografados e o domain security para o envio de e-mail entre organizações parceiras.

Portanto, este estudo fornece mecanismos favoráveis à obtenção de uma infraestrutura de e-mail robusta ao propor a utilização do Exchange Server 2010 como ferramenta de e-mail, onde se tem um ambiente estável de servidores de e-mail garantindo maior segurança nos dados. Permitiu o entendimento das vulnerabilidades e ameaças no ambiente de correio eletrônico e que é possível se implantar uma infraestrutura que as minimize, garantindo um ambiente seguro reduzindo a entrada de e-mails não solicitados, vírus e que se tenha controle e auditoria do que é administrado e a capacidade de manter a conformidade e atender os requisitos legais em relação às leis vigentes no país.

REFERÊNCIAS

Antispam.br. Disponível em: http://www.antispam.br/problemas/. Acesso em: 30 ago. 2012.

CAVALCANTI, Edjozane; FILHO, Walfredo; BRASILEIRO, Francisco. *Introduzindo Segurança no Correio Eletrônico Internet*. – Campina Grande – PB – Brasil. Disponível em: http://fubica.lsd.ufcg.edu.br/hp/publicacoes/artigos/ccb97.pdf. Acesso em: 10 nov. 2012.

Estatística de Notificações de Spam Reportadas ao CERT.br - valores acumulados: 2003 a dezembro de 2012. Disponível em: http://www.cert.br/stats/spam/. Acesso em: 16 fev. 2013

Exchange 2010 Help - *Database Availability Group Spans Two Sites*. Disponível em: http://www.microsoft.com/en-us/download/details.aspx?id=22392. Acesso em: 28 fev. 2013.

HOLME, Dan; RUEST, Nelson; RUEST, Daniele; KELLINGTON, Jason. *Configuring Windows Server 2008* Active Directory (2nd Edition). Washington: editora Bookman, 2011.

JAGOTT, Siegfriend; STIDLEY, Joel. *Microsoft Exchange Server 2010* Best Practices. Washington: editora Bookman, 2010.

KUROSE, James; ROSS, Keith. *Redes de Computadores e a Internet*: uma abordagem top-down. 3. ed. São Paulo: editora Person, 2006.

MCBEE, Jim; ELFASSY, David. *Mastering Microsoft Exchange 2010*. Indianapolis – Indiana: editora Wiley Publishing, 2010.

Microsoft Learning Team, 10135A *Configuring, Managing and Troubleshooting* Microsoft Exchange 2010.

Overview of Administrator Audit Logging, 2012. Disponível em: http://technet.microsoft.com/en-us/library/dd335052(v=exchg.141).aspx. Acesso em: 06 jan. 2013.

STALLING, William. *Criptografia e segurança de redes* – princípios e praticas. 4ª. Ed. São Paulo: editora Person, 2007.

STANEK, William. *Microsoft Exchange Server 2010* Administrator's Pockt Consultant. Washington: editora Bookman, 2010.

STANEK, William. *Microsoft Exchange Server 2003* Administrator's Pockt Consultant. Washington: editora Bookman, 2004.

TANENBAUM, Andrew. *Redes de Computadores*: 4ª. Ed. Rio de Janeiro: editora Campus, 2003.

Undertanding Active Manager. Disponível em: http://technet.microsoft.com/en-us/library/dd776123(v=exchg.141).aspx. Acesso em: 27 fev. 2013.

Understanding Header Firewall. Disponível em: http://technet.microsoft.com/en-us/library/bb232136.aspx. Acesso em: 10 nov. 2012.

Understanding Higt Availability and Site Resilience. Disponível em: http://technet.microsoft.com/en-us/library/dd638137(v=exchg.141).aspx. Accesso em: 27 fev. 2013.

Using a Database availability Group for Higt Availability. Disponível em: http://technet.microsoft.com/en-us/library/dd979799(v=exchg.150).aspx. Acesso em: 28 fev. 2013.