Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

MAICON DOS SANTOS SILVA

O VALOR DA INFORMAÇÃO: *PROXY* REVERSO – ForeFront TMG 2010

AMERICANA, SP

2012

Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

MAICON DOS SANTOS SILVA

O VALOR DA INFORMAÇÃO: *PROXY* REVERSO – ForeFront TMG 2010

Trabalho de conclusão de curso apresentado na Faculdade de Tecnologia de Americana, como parte das exigências do Curso de Tecnologia da informação para obtenção de titulo de Tecnólogo em Segurança da Informação.

Orientador: Prof. Carlos Henrique R. Sarro

AMERICANA, SP

2012

FICHA CATALOGRÁFICA elaborada pela

BIBLIOTECA – FATEC Americana – CEETPS

Silva, Maicon dos Santos

S581v O valor da informação: PROXY reverso – ForeFront TMG 2010. / Maicon dos Santos Silva. – Americana: 2012.

61f.

Monografia (Graduação de Tecnologia em Segurança da informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Me. Carlos Henrique Rodrigues Sarro

1.Segurança em sistemas de informação I. Sarro, Carlos Henrique Rodrigues II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Bibliotecária responsável Ana Valquiria Niaradi – CRB-8 região 6203

MAICON DOS SANTOS SILVA

O VALOR DA INFORMAÇÃO: *PROXY* REVERSO – ForeFront TMG 2010

Trabalho de conclusão de curso apresentado na Faculdade de Tecnologia de Americana, como parte das exigências do Curso de Tecnologia da informação para obtenção de titulo de Tecnólogo em Segurança da Informação.

Aprovado em quatorze de dezembro de 2012

Nota: 9,5

BANCA EXAMINADORA

Prof. Carlos Henrique R. Sarro (Orientador) – FATEC AM

Prof. Alexandre Garcia Aguado – FATEC AM

Prof. Rogério Nunes de Freitas– FATEC AM

AGRADECIMENTOS

Agradeço primeiramente a Deus, por me dar a vida e estar ao meu lado, me apoiando em todos os momentos.

Aos meus pais, agradeço por me proporcionarem tranquilidade e condições de hoje estar onde estou.

Ao meu orientador, Carlos Henrique Sarro, pelo suporte no pouco tempo que lhe coube, pelas suas correções e incentivos.

Agradeço os professores da Fatec por dividir seus conhecimentos e possibilitar meu desenvolvimento acadêmico e profissional.

Meus agradecimentos aos colegas de sala do curso de Segurança da Informação da FATEC, pelo apoio e companheirismo durante todo o curso.

Agradeço pelo apoio dos meus amigos de trabalho, pela disponibilidade quando precisei.

A minha noiva, agradeço por sempre estar ao meu lado, me incentivando e apoiando.

A todos que diretamente ou indiretamente fizeram parte da minha formação, muito obrigado.

DEDICATÓRIA

Dedico este trabalho a todos os profissionais de Tecnologia da Informação, pelas dificuldades encontradas no dia-a-dia, pela importância, cobrança e criticidade de nossas ações.

RESUMO

O objetivo deste trabalho é apresentar vários cenários possíveis para aplicação dos conceitos de *Proxy* e *Cache*, com foco na utilização do *Proxy* em sua tecnologia reversa, visando oferecer uma camada a mais na proteção dos servidores *web*. Após a apresentação da tecnologia, funcionalidades e exemplos de aplicações, o trabalho apresenta em sua conclusão a utilização do *Proxy* Reverso com a ferramenta da Microsoft ForeFront TMG 2010.

Palavras Chaves: *PROXY* REVERSO, *SERVIDOR WEB*, FOREFRONT TMG, *CACHE*, *WEB CACHE*, *PROXY*, *WEB PROXY*

ABSTRACT

The purpose of this work is to present several scenarios in order to apply concepts of Proxy and *Cache*, focusing on using Proxy in its reverse technology with the purpose of providing an additional layer on web servers protection. After the presentation of this technology, features and application examples, the work presents in its conclusion, the use of a Reverse Proxy with Microsoft ForeFront TMG 2010 tool.

Keywords: *PROXY* REVERSO, *WEB SERVER*, FOREFRONT TMG, *CACHE*, *WEB CACHE*, *PROXY*, *WEB PROXY*

LISTA DE ABREVIATURAS

CA – CERTIFICATE AUTHORITY

DMZ – DEMILITARIZED ZONE

FTP – FILE TRANSFER PROTOCOL

HTTP – HYPER TEXT TRANSFER PROTOCOL

HTTPS – HYPER TEXT TRANSFER PROTOCOL SECURE

IDS – INTRUSION DETECTION SYSTEM

IIS – INTERNET INFORMATION SERVICES

IP – INTERNET PROTOCOL

LAN – LOCAL AREA NETWORK

NAT – NETWORK ADDRESS TRANSLATION

RADIUS – REMOTE AUTHENTICATION DIAL-IN USER SERVICE

SSL – SECURE SOCKETS LAYER

TCP – TRANSMISSION CONTROL PROTOCOL

TI – TECNOLOGIA DA INFORMAÇÃO

URL – UNIFORM RESOURCE LOCATOR

LISTA DE FIGURAS

SUMÁRIO

OBJETIVO

Este trabalho tem como objetivo abordar a importância da informação para a organização, bem como apresentar configurações de segurança e topologias que podem ser implementadas a fim de proteger aplicações e servidores que dão acesso às informações coorporativas contra os constantes ataques de *hackers*[1] e à grande variedade de vírus distribuídos na rede mundial, a internet.

Para que este objetivo seja alcançado, a tecnologia denominada "*proxy* reverso" solução conhecida no mercado há alguns anos, porém não muito utilizada pelos administradores, será apresentada.

A solução *Forefront Threat Management Gateway* 2010 (TMG) foi escolhida para apresentação dos benefícios da tecnologia de *proxy* reverso, porém, este conceito se aplica a diversas outras aplicações disponíveis no mercado. Assim sendo, independentemente da ferramenta, o objetivo foi apresentar o que pode ser feito utilizando um servidor *proxy* independente.

É importante conscientizar o administrador que, com medidas simples, porém planejadas, muitas vezes disponíveis a nós, é possível criar barreiras e camadas de segurança mais robustas, oferecendo maior proteção para o negócio na organização, a informação.

[1] Hackers – Termo popularmente utilizado para fazer referência a uma pessoa que utiliza habilidades e conhecimentos avançados em informática para seu próprio proveito

INTRODUÇÃO

Atualmente presente na maioria das organizações, os ambientes de telecom[2] e tecnologia da informação possuem um cenário amplo e complexo, contendo diversas plataformas, aplicações e tecnologias diferentes.

> *"À medida que a revolução digital continua a transformar o panorama dos negócios, organizações bem-sucedidas devem sustentar seus lucros em um mercado global altamente competitivo e em rápida mudança, sobrevivendo a uma política mundial que muda seus mercados fontes de mão-de-obra."* (TURBAN, RAINER e POTTER, 2005)

A administração destas tecnologias e plataformas distintas são os grandes desafios encontrados pelos analistas de TI[3] e responsáveis pela administração do ambiente computacional da empresa, que a cada dia tendem, com maior frequência, procurar por soluções rentáveis e funcionais para garantir a operacionalidade do ambiente, mantendo ou aumentando a segurança.

> *"A tecnologia da informação oferece as ferramentas que permitem as pessoas na organização solucionar problemas cada vez mais complexos e aproveitar as oportunidades que contribuem para o sucesso, ou mesmo a sobrevivência da organização." (*TURBAN, RAINER e POTTER, 2005*)*

Devido à necessidade constante pela disponibilidade da informação, a solução adotada pelas organizações é a portabilidade na disponibilização da informação, fazendo com que grande parte destas informações encontradas em aplicações sejam desenvolvidas de modo a executá-las em um ambiente *web*, ou seja, em um servidor *web*, disponibilizando o acesso a partir de qualquer terminal que tenha suporte ao protocolo HTTP[4].

[2] Nome utilizado no meio tecnológico em abreviação a palavra: Telecomunicações
[3] TI – Tecnologia da Informação: Analistas, técnicos, pessoas que trabalham com tecnologia
[4] HTTP - Hyper Text Transfer Protocol – é um protocolo de comunicação utilizado para sistemas de informação de hipermedia distribuídos e colaborativos.

Com a necessidade de melhorar e automatizar seus processos, o aumento do número de aplicações dentro de uma organização é uma tendência do mercado atual, constituindo-se em uma das metas a ser conquistadas.

Existem várias opções de ferramentas disponíveis no mercado para desenvolvimento de aplicações *web*. Estas aplicações podem funcionar como *web site* informativo de acesso público (a partir de toda a internet), *web site* ou portal corporativo, com acesso restrito e interno de colaboradores de uma determinada organização, ou a combinação destas duas opções, sendo um portal de acesso público e restrito.

> *"Muitas grandes empresas já implementaram portais corporativos para reduzir custos, ganhar tempo para executivos e gerentes ocupados e melhorar a lucratividade. Além disso, portais corporativos oferecem aos clientes e funcionários oportunidade de auto-atendimento. As maiores aplicações de portal incluem oferecer bases de conhecimento e ferramentas de aprendizado; suporte ao processo empresarial; e vendas, marketing e suporte voltados para o cliente."* [TURBAN, RAINER e POTTER, 2005]

Dentro de uma organização, principalmente partindo da segurança da informação, a padronização de uma tecnologia para desenvolvimento e utilização de aplicações *web* fica muito difícil. É neste cenário que a administração destas plataformas e servidores de tecnologias diferentes se torna complicada e ariscada.

É na dificuldade de administrar um ambiente de plataformas e tecnologias diferentes que este trabalho se posicionará, executando aplicações *web* e mantendo este ambiente seguro e atualizado.

JUSTIFICATIVA

As empresas estão cada vez mais dependentes da disponibilidade de informações a fim de prestar serviços aos clientes. Uma gestão eficaz de informação requer o desenvolvimento de um ambiente no qual as informações possam ser fornecidas a qualquer pessoa autorizada, em qualquer lugar e em qualquer tempo (GIBB, BUCHANAN, 2006).

Ter a segurança em disponibilizar um recurso ou informação de valor para a organização aliado a tecnologia da informação é a peça fundamental para o sucesso de um negócio.

1. O VALOR DA INFORMAÇÃO

Neste capítulo, abordaremos a importância da informação para a organização e para a continuidade do negócio, explorando dados estatísticos de acordo com a pesquisa referenciada.

1.1 Informação

Conforme definição dos dicionários, (AURELIO, 2010) (MICHAELIS, 2010) **informação** é uma palavra derivada do latim informatio + onis, Acto ou efeito de informar, Notícia (dada ou recebida), Esclarecimento dado sobre os méritos ou estado de outrem.

> *"Uma empresa em atividade é, por natureza, um sistema aberto e interativo suportado por uma rede de processos articulados, onde os canais de comunicação existentes dentro da empresa e entre esta e o seu meio envolvente são irrigados por informação. (Ascenção Braga, 1996)"*

Costumamos tomar como bem de valor somente algo físico e tocável, porém, com o aumento da informatização no mundo corporativo, o conceito de valor acaba ganhando outros sentidos.

Gurgel (2006) afirma que:

> *"Atualmente, a informação tem sido considerada como o principal bem que uma organização possui. Apesar de o seu valor está sendo visualizado com maior atenção nos dias atuais, a informação está presente em cada época da história representando diferentes papéis, e que por muitas vezes não foi tratada como crucial para a sobrevivência das organizações.(Gurgel; Giovane, 2006).*

Dentre as mais variadas descrições da importância da informação, quando comparadas aos dados e afirmações, a conclusão e a mesma: trata-se de um bem muito valioso e crítico de se manipular.

De acordo com Ascenção (1996),

> *"À escala das organizações, a informação é um fator decisivo na gestão por ser um recurso importante e*

> *indispensável tanto no contexto interno como no relacionamento com o exterior. Quanto mais fiável, oportuna e exaustiva for essa informação, mais coesa será a empresa e maior será o seu potencial de resposta às solicitações concorrenciais. Alcançar este objetivo depende, em grande parte, do reconhecimento da importância da informação e do aproveitamento das oportunidades oferecidas pela tecnologia para orientarem os problemas enraizados da informação."*

Baseando-se nisto fica evidente a importância em se obter planos de conscientização dos recursos empresariais, definindo responsabilidades e deveres de cada funcionário, colaborador, prestador de serviços e integrante da corporação. Procurar a melhoria constante dos processos de segurança da informação deve ser uma meta.

Ainda, Dawel (2006) afirma que:

> "*Um dados divulgado por analistas de mercado em uma conferência sobre segurança revelou que 84% dos incidentes de segurança vem de dentro da empresa, e apenas 16% são de origem externa. Em geral, tratam-se de pessoas, funcionários ou terceiros que estão, ou pelo menos deveriam estar comprometidos com o sucesso da empresa e o atendimento dos objetivos corporativos."*

Tomando-se como exemplo um funcionário que tem acesso a todos os recursos da rede da empresa a partir de sua residência; este se encontra no ambiente "externo", porém com acesso a recursos como se estivesse sentado em sua estação de trabalho dentro do escritório (ambiente interno).

Outro exemplo é um sistema empresarial, seja de vendas ou de consulta de informações disponível para acesso na *WEB*, onde se deve ter total controle deste acesso, a fim de garantir o acesso somente autorizado, dado o grau de criticidade de determinadas informações para o negócio.

Dada à importância do valor das informações no âmbito de qualquer instituição, deve-se levar em consideração os três pilares básicos da segurança da informação: Confidencialidade, Integridade e Disponibilidade [NBR ISO/IEC-17799].

1.1.1 Confidencialidade

É a garantia de que o acesso às informações seja obtida somente por entidades autorizadas.

A confidencialidade pode ser classificada em níveis de acordo com as necessidades da empresa, podendo ser:

1) Confidencial

Pode ser manipulada por um número reduzido de pessoas ou um setor da empresa, como por exemplo P&D[5];

2) Restrita

Informação restrita pode ser manipulada por contingente maior de pessoas ou um nível hierárquico, como por exemplo o plano estratégico da empresa, podendo ser visto até mesmo pelo nível hierárquico de diretoria;

3) Interna

Este tipo de informação deve ser limitada à empresa, como as listas de ramais, memorandos internos, norma internas, manuais, etc.;

4) Pública

Estas informações podem também ser divulgadas ao público ou publicadas em revistas, sites, etc. Informações públicas podem também ser conhecidas como 'não classificadas', pois se entende que, se não foi classificada é porque é pública. Isso pode trazer vários e sérios problemas para a empresa, pois a falha de classificação pode expor informações confidenciais ao público. Adotar que tudo o que não é classificado é interna, seria o mais seguro a fazer.

1.1.2 Integridade

É a Garantia de que as informações serão protegidas contra alterações não autorizadas, mantendo exatidão e inteireza das mesmas, tal qual como foi armazenada e disponibilizada;

[5] P&D – Setor de pesquisa e desenvolvimento da organização ou empresa.

Um dado ou informação armazenado deve permanecer íntegro para quando for recuperado. Para que isso seja verdadeiro, não poderá sofrer interferência alguma que o modifique, seja por falhas intencionais ou não. Os métodos de processamento, normalmente sistemas, devem também ter a integridade preservada, pois uma alteração num sistema pode comprometer as informações resultantes do processamento. Este conceito não garante que os dados estejam corretos, pois se forem armazenados errados, assim permanecerão até que uma entidade autorizada os corrija.

1.1.3 Disponibilidade

É a garantia de que as informações estarão disponíveis onde e quando as entidades autorizadas necessitarem, com total segurança.

A informação não tem valor para a empresa caso não esteja disponível quando for requisitada. Muitos ataques tentam derrubar este pilar da segurança por meio da negação de serviço, com ataques do tipo *DoS*[6] ou *DDoS*[7], interrompendo o acesso aos serviços e informações das empresas. Para que este problema seja apresentado, não é necessário ataque sofisticado, bastando para isso apenas que uma linha de comunicação seja interrompida ou que um servidor seja fisicamente comprometido, intencionalmente ou não. A falta de energia que alimenta o servidor de dados pode causar indisponibilidade, caso não haja contramedidas para este problema. A manutenção destes pilares da segurança da informação só será atingida se houver a integração entre segurança física e do ambiente, tecnológica e em pessoas.

> *"Sabendo que a informação armazenada nos computadores da empresa ou em outros meios possui um alto valor para a continuidade dos negócios, o profissional de segurança deve se preocupar com o todo. A visão empresarial deve ser um pré-requisito de qualquer profissional, isso inclui o de segurança da informação."* (George Dawel, 2005)

Como pôde ser observado, a atenção deve ser dada não somente para parte tecnológica, mas também aos processos definidos para acesso a informação e sua utilização consciente e responsável.

[6] DoS - Denial of Service: Ataque de negação de serviço na tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores.
[7] DDoS - Distributed Denial of Service: Ataque distribuído de negação de serviço

1.2 Continuidade do Negócio

Dawel (2005) afirma que:

> *"Uma informação dada pelo U.S. Small Business Administration e divulgada na Insight Magazine dá conta que 43% das empresas e médias empresas nunca reabrem após sofrer um desastre, e que 29% fecham em dois anos. É um dados assustador, pois somados são 72% das empresas que não conseguem superar e sobreviver a um evento como esse."*

A informação e o conhecimento são os bens mais preciosos de uma empresa para a continuidade do negócio, portanto, devem ser claros os meios de segurança e proteção deste bem.

Tomando como exemplo uma empresa de vendas de produtos automotivos, como óleo para motores, que disponibilizam informações sobre seus catálogos de produtos na *web* para acesso de vendedores externos, clientes e diretores; tais informações podem apresentar um prejuízo imensurável para o negócio, caso seja divulgada na internet ou que sua concorrente tenha acesso à mesma.

Este cenário pode apresentar um grande risco para continuidade do negócio, levando em consideração o seguimento de cada empresa e o tipo de informação trabalhada.

Com auxílio da tecnologia, aliada aos processos de gerencia de pessoas, é possível minimizar os riscos, mitigando e analisando as vulnerabilidades do ambiente de trabalho. Veremos no capitulo 2, uma tecnologia que traz grande auxílio no controle de informações e na segurança do ambiente empresarial.

2. *PROXY* E *CACHE*

Neste capítulo abordaremos as tecnologias usadas no meio empresarial no intuito de ter um maior controle do ambiente operacional da empresa e da organização.

2.1 O que é *Proxy*

Gallo, Michael A. e HANCOCK, WILLIAM M (2003) afirmam que:

> *"Proxy é um programa de aplicação intermediário que age como servidor e cliente; ele é usado como um representante para a aplicação. Nas especificações do HTTP, um proxy é considerado como um agente de reenvio. Ele recebe pedidos por um URL e reescreve toda ou parte da mensagem original e reenvia essa mensagem formatada ao servidor especificado no URL."*

Ainda conforme Gallo e HANCOCK (2003):

> *"Um uso comum do proxy é quando um cliente está por trás de um firewall. Neste caso, uma conexão é estabelecida entre o cliente e o proxy e entre o proxy e o servidor origem. Os pedidos de cliente e as respectivas respostas do servidor são submetidos ao proxy, que os repassa ao servidor e cliente, respectivamente."*

Baseando-se nos autores citados, o *proxy* está presente na maioria de nossos acessos, porém, disponível de diversas formas diferentes.

De acordo com TURBAN, RAINER e POTTER (2005) tem-se outra definição:

> *"Proxy (traduzindo-se: procuração) funciona como um intermediário entre os usuários que precisam acessar páginas das internet e os servidores dessas páginas. Este é um serviço de rede que pode ser posicionado na DMZ. Assim, quando um usuário solicita uma página ao Proxy, e isso é feito de forma transparente, o Proxy verifica se já possui a página requisitada em sua área de armazenamento (conhecida como Cache) e se o conteúdo da página não está expirado. Cumpridas essas*

condições, o Proxy não acessa a internet e transfere ao usuário a que está no cache ; caso contrario, busca a página na internet e transferi-la ao solicitante."

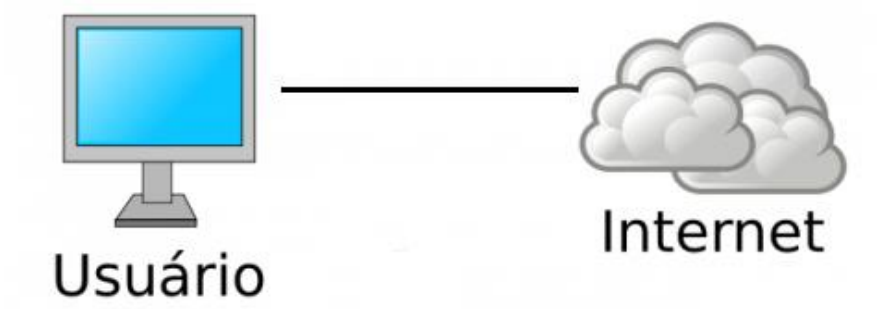


Figura 1. Topologia de rede. Não há adoção de um servidor *Proxy* para navegação *web* (SOLUÇÕES, 2012).

Para exemplificação, como demonstrado na Figura 1, temos um exemplo de acesso comum à internet, ou seja, sem um p*roxy* intermediando o acesso ao conteúdo da *WEB*.

Conforme classificação de TANENBAUM:

> *"Um servidor proxy é um tipo de gateway que comunica em HTTP com o browser e em FTP, Gopher ou outro proto com o servidor. Ele aceita solicitações em HTTP e as traduz para solicitações FTP, por exemplo, de modo que o browser [8]não necessite compreender nenhum protocolo que não o HTTP. O servidor proxy pode ser executado na mesma máquina do browser, mas também um estar em uma outra máquina em algum ponto da rede e servindo à via browsers.*

Além de funcionar como um tradutor para protocolos desconhecidos, os servidores *proxy* têm várias outras funções, como, por exemplo, *cache*[9]. Um servidor *proxy* que funciona como *cache* armazena todas páginas que passam por ele. Quando um usuário solicita uma página servidor *proxy* verifica se a tem. Se a tiver, o servidor poderá verificar se a página

[8] Browser – aplicação que permite o acesso a sites da internet

[9] *Cache*- é um dispositivo de acesso rápido, interno a um sistema, que serve de intermediário entre um operador de um processo e o dispositivo de armazenamento ao qual esse operador acede.

ainda é atual. Se a resposta for afirmativa, a página é transmitida o usuário. Caso contrário, o *browser* [10]busca outra cópia na *Web*.

Por fim, algumas organizações podem posicionar o servidor *proxy* em seu *firewall* para garantir aos usuários acesso à *Web* mas sem dar a eles acesso total à Internet. Nesse tipo de configuração, os usuários podem se comunicar com o servidor *proxy*, mas é o servidor *proxy* que faz contato com os sites remotos e busca as páginas para seus clientes. "Esse mecanismo pode ser usado, por exemplo, por escolas, para bloquear o acesso aos sites da Web considerados impróprios." (TANENBAUM, 1999).

A Figura 2 representa o oposto daquela representado pela Figura 1. Nela, é possível observar o acesso a internet realizado através de uma rede que se utiliza Proxy.

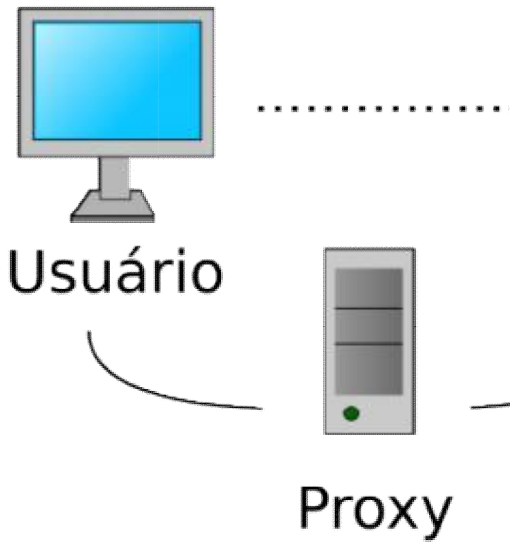


Figura 2. Representação de uma topologia de rede que faz uso do servidor *Proxy* para navegação na *web* (SOLUÇÕES, 2012)

É visível que o *proxy* funciona como uma camada a mais de proteção no acesso a internet, centralizando todos os acessos internos ao ambiente externo.

[10] *Browser* – aplicação/programa utilizado para acesso a sites da internet

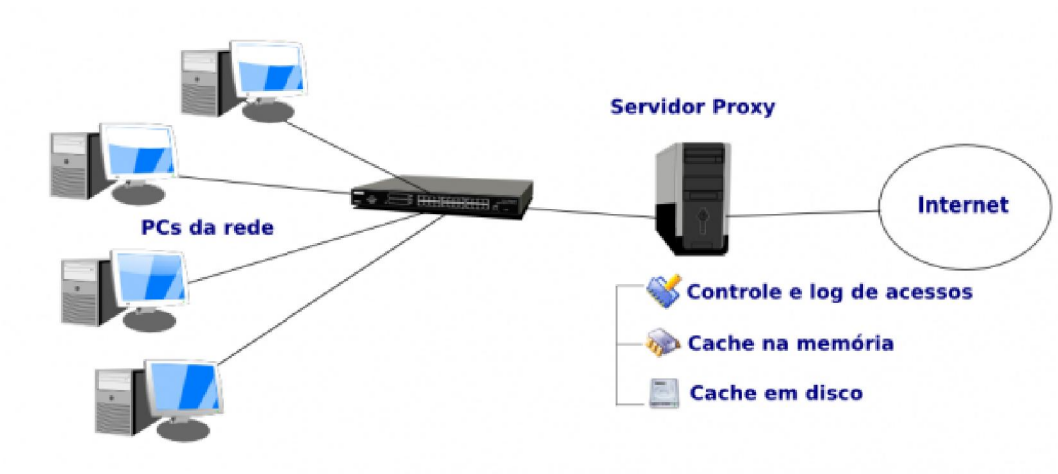


Figura 3. Uso de servidor *Proxy* para navegação na *web* (MACEDO, 2012)

Conforme pode ser observado na Figura 3, uma rede que utiliza servidor *proxy* para acesso a *web*, tem a possibilidade de realizar o balanceamento do acesso a *web*, mantendo maior controle dos acessos e proporcionando mais agilidade e confiabilidade.

Dentre as possibilidades de configurações, veremos no capitulo a seguir os diferentes tipos de *Proxy* disponíveis para utilização no ambiente empresarial, educacional e até mesmo residencial.

2.2 Principais Tipos de *Proxy*

Assim como as demais tecnologias, existem diversos tipos de *Proxy* disponíveis para aplicação em vários seguimentos, como por exemplo: Educacional, Empresarial e Residencial.

Abaixo, será apresentado os principais tipos de *Proxy* e suas utilidades.

2.2.1 Proxy Web

É o tipo mais comum, conforme definido na introdução deste capitulo. Chamado de *Web Proxy Cache*, armazena páginas *Web* e arquivos disponíveis em servidores *web* remotos, aumentando a agilidade e confiabilidade do acesso de clientes da rede local.

Utilizando um algoritmo de expiração, quando recebe uma requisição de acesso a algum recurso da *web*, o *proxy cache* verifica se o recurso está armazenado em *cache*, verificando se está expirado ou não, em caso contrario, efetua a busca do recurso na *web*, armazenando localmente e realizando a entrega do recurso ao usuário.

Alguns dos algoritmos de expiração utilizados são:

- LRU (Least Recently Used) é um algoritmo de substituição de página que apresenta um bom desempenho substituindo a página menos recentemente usada. Esta política foi definida baseada na seguinte observação: se a página está sendo intensamente referenciada pelas instruções é muito provável que ela seja novamente referenciada pelas instruções seguintes e, de modo oposto, aquelas que não foram acessadas nas últimas instruções também é provável que não sejam acessadas nas próximas;
- FIFO *(First-in, First-out)* é um algoritmo de substituição de páginas de baixo custo e fácil implementação, pois consiste em substituir a página que está a maior tempo na memória. Porém está escolha não verifica se a página, mesmo tendo entrado primeiro na memória, está sendo muito utilizada ou não, o que pode prejudicar o desempenho do sistema. Por esta razão, não se utiliza o FIFO puro, ou seja, sem complemento de outros algoritmos; (TANENBAUM, 1999)
- LFU (*Least Frequently Used*) — menos frequentemente utilizado. Remove o objeto menos popular, porém não considera tempo do último acesso. Considera o número de acessos. Problema: o *cache* pode ficar com objetos muito acessados e velhos;
- GDS (*Greed Dual Size*) –. Atribuí valores baseados no custo de um hit para os objetos armazenados no *cache*. O custo pode ser latência ou pacotes transmitidos pela rede. São mantidos em *cache* objetos menores, referenciados mais vezes. (Maziero, Carlos, 2010).

2.2.2 Proxy transparente

Muitas organizações implementam o *proxy* no intuito de reforçar a segurança no uso da rede e melhorar o acesso a *web* através do *cache*, porém, usuários com algum conhecimento de informática conseguem burlar esta configuração, retornando a configuração original do *browser*, deixando de utilizar o servidor *proxy*.

Neste cenário, a utilização do *proxy* transparente ou o *transproxy* efetua uma combinação de *NAT*[11] com servidor *proxy* sem a necessidade de efetuar configurações adicionais e nas estações dos usuários.

Dentre as soluções de *proxy* transparente, pode-se destacar o protocolo WCCP [12] implementado pelos roteadores da CISCO[13]. As grandes corporações sempre possuem um

[11] Nat - Network Address Translation - é uma técnica que consiste em reescrever os endereços IP de origem de

roteador para servir de *front end* [14]para a Internet e este seria apenas mais um serviço a ser implementado. O WCCP se mostra uma solução interessante, visto que ele permite redundância e balanceamento de carga de servidores *proxy*, e, no caso de falha em todos os servidores, permite a saída direta para a Internet. (Menezes, 2002)

2.3 Vantagens

Com a utilização de service *Proxy* ou servidor, temos disponíveis para utilização vários recursos, conforme citado por *Techwan (2012*). Exemplificando, pode-se citar a criação de grupos:

- Grupo A - Acessa somente site do governo (gov.br);
- Grupo B - Acessa site do governo (gov.br) e (.com.br);
- Grupo C - Acessa todos os sites.

Mais alguns recursos do *proxy*:

- Bloqueio sites por URL ou IP;
- Bloqueio sites por palavras chaves;
- Bloqueio sites pelo conteúdo da página;
- Relatório por estação;
- Relatório de *downloads*;
- Bloqueia *downloads*;
- Bloqueia sites por hora;
- Bloqueia sites por data;
- Bloqueia *downloads* de arquivos com suspeita de vírus;
- Bloqueio de tudo e liberação somente de sites permitidos;
- Libera tudo e bloqueia os sites proibidos.

Pode-se dizer que há dois grandes motivos pelo qual se deve utilizar um *proxy*/*cachê*. Sendo estes motivos simplificados a baixo.

2.3.1 Controle de acesso

Com a internet cada vez mais acessível a pequenas e médias empresas, um número imenso de pessoas está se interligando a internet. Isso faz com que as pessoas tendam a passar

[12] WCCP – Web *Cache* Cordination Protocol
[13] Cisco – empresa fabricante de equipamentos de rede
[14] Front end: refere-se ao estagio inicial de um fluxo de processo.

mais tempo navegando por sites não relativos ao seu trabalho primário, acessando sites que não condizem com a política da empresa. Exemplificando, a utilização de sites de relacionamento como ***Twitter***, ***Orkut*** e ***Facebook***[15] vem crescendo e, consequentemente, poderá vir a atrapalhar o usuário em cumprir suas funções dentro da empresa. Ainda, pode haver uma ameaça sempre presente de propagação de *downloads* de softwares piratas e músicas, fatores que podem complicar a vida de uma empresa durante fiscalizações e auditorias. (MOVE WAY IT, 2012)

2.3.2 Desempenho

Visando aproveitar ao máximo essa banda de qualidade, a utilização de *proxy*/*cache* torna-se quase que obrigatória. Ainda de acordo com a Rede Nacional de Ensino e Pesquisa (RNP) - 2, a utilização de *proxy*/*cache* pode gerar uma economia entre trinta e cinquenta por cento nos horários de pico. Isso significa que para um link de 2 Mbps que está operando a plena carga e considerando uma redução de 30 %, o mesmo produziria um ganho na banda agregada de aproximadamente 600 Kbps. Ou seja, a simples implementação de um *proxy*/*cache* bem ajustado gera uma economia da ordem de milhares de reais por mês para a empresa. (Linux Ponta, 2012).

Funcionam como firewall e filtro de conteúdo: constituem um mecanismo de segurança implantado pelo provedor de Internet ou pelos administradores da rede em um ambiente de intranet a fim de desativar o acesso ou filtrar solicitações de conteúdo de determinados sites considerados ofensivos ou prejudiciais para a rede e os usuários.

Melhoram o desempenho, pois armazenam em *cache* as páginas da Web acessadas por hosts da rede durante determinado período. Sempre que um host solicita a mesma página da Web, o servidor proxy utiliza as informações armazenadas em *cache* em vez de recuperá-las do provedor de conteúdo. Isso proporciona acesso mais rápido às páginas da Web.

Alterando o posicionamento do servidor *proxy* na topologia de rede, é possível utilizá-lo em conjunto com um *firewall* para proteger, de forma mais específica, servidores *web* com conteúdo HTTP, HTTPS e FTP[16], maiores informações sobre este recurso no capitulo 3 *Proxy* Reverso.

Portanto, como observado anteriormente, as vantagens na utilização de um servidor *Proxy* são inúmeras, auxiliando na administração da segurança, controle de acesso e desempenho do ambiente empresarial.

[15] Twitter, Orkut, Facebook – São sites de relacionamento, ou como conhecido popularmente, redes sociais disponíveis da internet

[16] FTP - File Transfer Protocol. É um protocolo usado para transferir arquivos através de redes TCP/IP

2.4. O que é *Cache*

A quantidade de informação disponível na Internet aumenta a cada dia. O comércio eletrônico, *home banking*[17], compras *on-line*[18], propaganda, redução nos custos de acesso à Internet e acessos gratuitos, tem se agravado cada vez mais os gargalos nas conexões. "Recursos como o uso de *cache* de *Web* têm sido implantados para reduzir o tráfego, de forma que se evite a utilização de conexões da Internet, diminuindo o tempo de acesso e aumentando a qualidade do serviço para os usuários finais. (OLIVEIRA, 2002)

A quantidade de dados que trafegam na internet aumenta cada a cada dia, pois com a acessibilidade e a utilização como um dos principais meios de comunicação, pesquisa, marketing e entretenimento, a má utilização deste meio e a falta de planejamento podem trazer consequências negativas para as organizações, como lentidão e até indisponibilidade. Exatamente para este cenário que o conceito de *cache* foi criado.

O armazenamento em *cache* é uma tecnologia usada por diversos aplicativos e dispositivos de hardware, que utilizam a memória *cache* para armazenamento de instruções utilizadas com maior frequência, a fim de acelerar as tarefas de processamento. (OLIVEIRA, 2002)

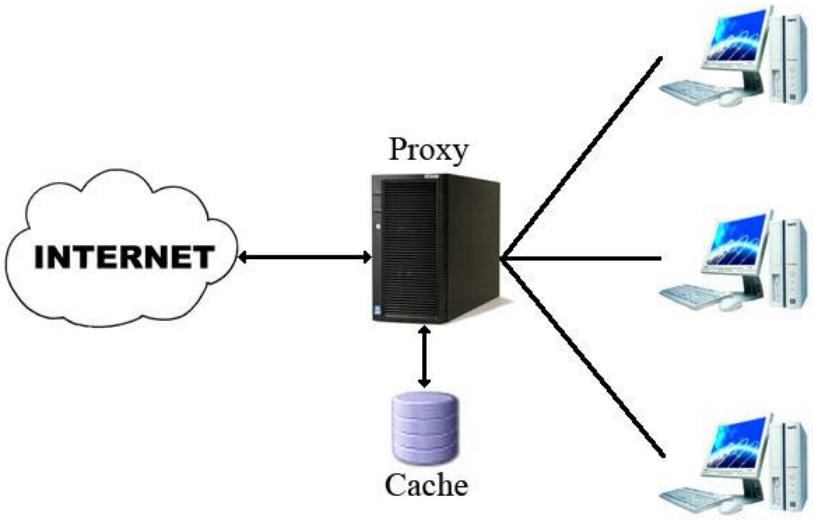


Figura 4. Topologia de rede que faz uso do *Cache* para navegação na *web* (INCON, 2012).

[17] Home Banking – Portal de transações bancarias disponibilizado aos seus clientes por bancos, instituições financeiras

[18] Online – Conectado a internet, por meio/através da internet.

Conforme Oliveira (2002), para armazenamento em *cache* da *web*, o mesmo conceito é aplicado, embora de maneira mais ampla, usando-se um servidor ou dispositivo especializado.

Os documentos requisitados são copiados em posições mais próximas do usuário com o intuito de diminuir o tempo do próximo acesso ao documento.

Utilizar *cache*s na *web* significa armazenar cópias de documentos muito acessados em servidores mais próximos aos clientes, o que diminui tanto a carga na rede como as requisições feitas a servidores que possuem documentos muito populares. Como resultado, o usuário experimenta uma diminuição do tempo de resposta a requisições feitas.

2.5 Tipos de Cache

De acordo com Cláudia Shizue Watanabe um serviço de *cache* pode ser classificado segundo os tipos:

2.5.1 Browser Cache

A maioria dos visualizadores possui um *cache* próprio, pois é bastante provável que um usuário acesse as mesmas páginas frequentemente ou até mesmo num mesmo dia. *Browser Cache*s não são compartilhados entre os usuários.

2.5.2 Proxy Cache

Pode ser acessado e compartilhado por muitos usuários. A aplicação *proxy* age como intermediário entre clientes e servidores WWW[19]. O servidor local procura pela página, grava-a no disco e repassa para o usuário. Requisições subsequentes de outros usuários recuperam a página que está gravada localmente. Os servidores *proxy*s são usados por organizações ou provedores que querem reduzir a quantidade de banda que utilizam.

2.5.3 Transparente Proxy Cache

É assim chamado porque ele trabalha interceptando o tráfego da rede transparentemente para o *browser*. São usados especialmente por *ISP*[20], porque não é necessária nenhuma configuração no *browser* do usuário. (WATANABE, CLÁUDIA, 2000)

2.6 Vantagens

Pode-se citar como vantagens do uso de servidores *cache*:

[19] WWW- Tradução World Wide Web (Web ou www) é uma rede de computadores na Internet que fornece informação em forma de hipertexto

[20] ISP - Internet Service Provider - é uma empresa que fornece acesso à Internet.

- Redução do tráfego: Menos requisições e respostas precisam trafegar na rede. O objeto é recuperado do servidor somente uma vez, reduzindo a quantidade de banda usada pelo cliente. Pode-se conseguir taxas de acerto de até 60%;
- Redução de carga dos servidores: Menos requisições para o servidor WWW atender. Exemplificando, alguns sites ficam extremamente congestionados quando do lançamento de novos produtos. Um servidor *proxy* pode resolver o problema;
- Redução da latência: As respostas de requisições aos objetos "*cache*ados" são feitas a partir do *cache* local, não pelo servidor WWW original, ou seja, o acesso tende a ser bastante rápido;
- Possibilidade de acesso: Considerando que o servidor WWW do endereço especificado no URL está inacessível (queda de enlace, servidor desligado, etc) ou está recebendo mais solicitações do que ele pode aguentar, se a página estiver armazenada no *proxy* será possível acessá-la. (WATANABE, CLÁUDIA, 2000).

2.7 Critérios

A parte dinâmica do conteúdo *web* não deve ser armazenada em sistemas de *cache* (exemplos: programas *CGI (Common Gateway Interface*) utilizados para consultas à alguma base de dados, páginas que registram a data atual ou contadores de acesso dentre outros.

Devem ser incluídos no cabeçalho dos pacotes, comandos e formatos de mensagens HTTP para que o sistema *cache* saiba qual conteúdo deverá ou não armazenar: [RFC 2616, 1999]. Exemplificando:

- *Public*: indica que o conteúdo pode ser armazenado em qualquer sistema de *cache*;
- *Private*: indica que todo o conteúdo ou parte dele é de interesse de um usuário único, este conteúdo não deve ser armazenado em um sistema de *cache* compartilhado. Somente um *cache* privado (por exemplo, o *browser* do usuário) poderá armazenar este tipo de conteúdo;
- *No-cache*: indica que sempre que o conteúdo for solicitado, deverá ser enviado pelo servidor original e não pelo *cache*. O conteúdo não é armazenado em *cachê*.

3. *PROXY* REVERSO

Neste capítulo será abordado o assunto e tecnologia principal apresentados neste trabalho. O Proxy reverso será apresentado em suas diversas configurações, explorando pontos de vantagens e comparativos.

3.1. O que é *Proxy* Reverso

Proxy reverso é a tecnologia usada para reduzir a carga em um servidor *web* usando *cache* entre o servidor e a Internet. Pode ser implantado com autenticação, atuando como uma camada a mais na segurança do acesso. Um bom exemplo de uso do *Proxy* reverso é aliviar a carga em um servidor *WEB* que fornece conteúdo estático e dinâmico. O conteúdo estático pode ser armazenado no *cache* do *Proxy* reverso, fazendo com que o servidor *web* consiga dar melhor responder de forma mais rápida e eficiente às requisições de conteúdo dinâmico. (SILVA, 2010)

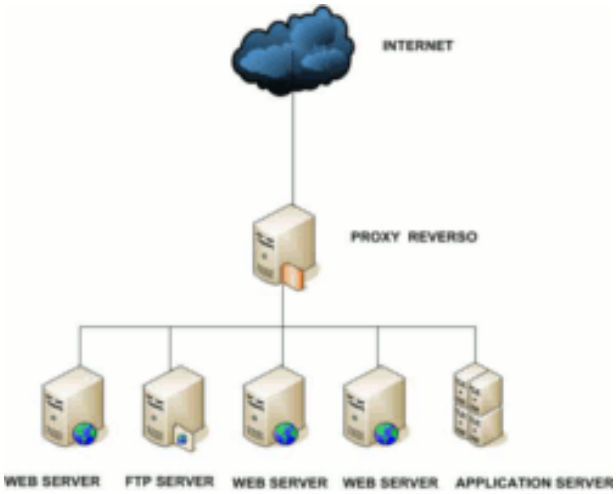


Figura 5. Representação de uma topologia de rede que faz uso do *Proxy* reverso (SILVA, 2010)

A figura 5 exemplifica o uso do *Proxy* reverso intermediando o acesso a aplicações e *web severs*.

Como o *Proxy* reverso realiza a interface entre a rede interna de servidores e a internet, é possível implementar controles de acessos baseados em certificados digitais, autenticação com usuário interno de um controlador de domínio e balanceamento de carga, realizando a distribuição no acesso aos servidores.

Ao contrário do *Proxy* comum, o cliente externo não necessita realizar configurações específicas para realizar o acesso ao *Proxy* reverso. É possível criar uma URL personalizada para acesso ao conteúdo, sem expor o servidor de origem e a rede local na internet.

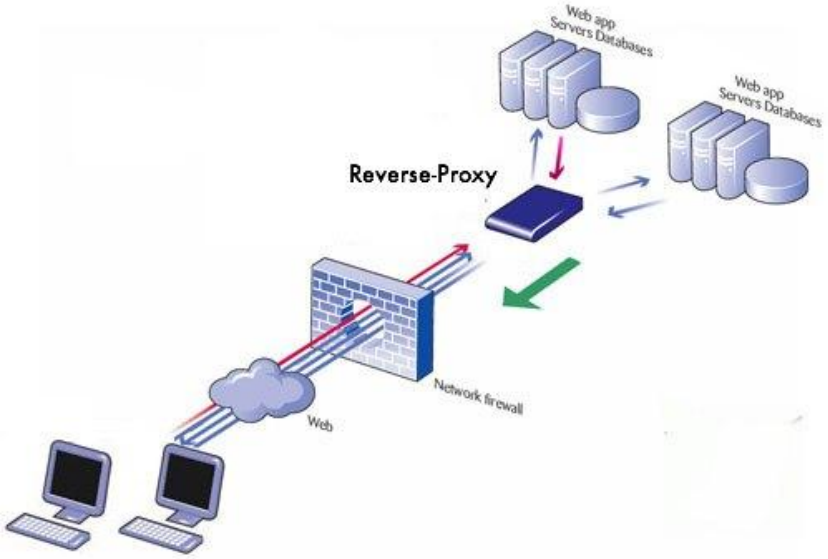


Figura 6. Aplicação do *Proxy* reverso no balanceamento do acesso (ZHOU, 2011)

Como pode ser observado na Figura 6, o *Proxy* reverso fica entre a internet e o servidor *web*, interceptando todas as requisições direcionadas ao servidor *web* controlando o trafego antes que ele possa alcançar o servido. Este método funciona semelhante à aplicação interna do *Proxy*, ou seja, realiza uma consulta do serviço requisitado ao *cachê* e, se estiver disponível, responde a solicitação de origem com o conteúdo resgatado, ou direcionado ao servidor para obter a informação, no caso de conteúdo dinâmico.

3.2 *Proxy* reverso como servidor *web*

É preciso que o *Proxy* reverso trabalhe como um servidor *web* para que possa tratar as requisições originadas da internet e repassá-las aos servidores *web* que estão na rede interna. Deve ser capaz de omitir informações referentes à rede local e aos servidores conectados a ela, para as maquinas clientes de acesso externo, ou seja, da internet.

Como trabalho semelhante feito pelo *Proxy* convencional, o *Proxy* reverso oculta para a internet informações pertinente às maquinas da rede interna.

As máquinas clientes, que estão na Internet, se conectam ao servidor *proxy* reverso como se ele fosse o próprio servidor *web* e o redirecionamento para o verdadeiro servidor *web* é realizado de maneira transparente pelo *proxy*, para a máquina cliente.

3.3. Funcionamento do *Proxy* Reverso

O *Proxy* reverso funciona como um servidor *WEB* atuando como ponto único de acesso de um determinado serviço, aplicativo ou site *web*, porém, para as máquinas clientes na internet, este acesso é transparente (COAT, 2005).

Atuando como principal meio de acesso, é possível camuflar o endereço original de onde o serviço encontra-se hospedado e funcional, tornando assim uma barreira a mais na segurança do acesso. Através deste acesso centralizado, pode-se ter um maior controle quanto ao fluxo de requisição, monitoramento e configurações de segurança.

Para que atue como "falso servidor *web*", o *Proxy* reverso precisa fazer o direcionamento correto das interações e requisições para os verdadeiros servidores *web*, seguindo as seguintes atividades:

- A máquina cliente realiza a requisição ao *Proxy* Reverso assumindo que ele é o próprio *web server*. Para que o *Proxy* reverso interprete o cabeçalho HTML e realize o direcionamento para o *web server* interno, é necessário que seja realizado o mapeamento da URL para que ela seja convertida na URL real do *web server* interno. Responsável por transportar o *hostname* e o número da porta do host que hospeda o serviço solicitado, o campo host do cabeçalho HTTP precisam também ser mapeado e reformulado, para que faça a referencia correta ao serviço internamente. [RFC2616, 2007];
- Os campos dos pacotes de resposta também são passiveis de revisão, pois na resposta do *web server* ao *Proxy* reverso para que o cliente possa receber a informação correta, um dos campos a serem reconfigurados é o campo "*location"*, no cabeçalho HTTP é responsável transportar e armazenar a localização dos arquivos dentro do servidor. (RFC2616, 2007].

Com intuito de melhorar a segurança do acesso, existem diversas opções que quando combinadas entre si, garantem maior segurança no acesso mantendo o maior número de registros, tanto de acesso quanto de conteúdos a transitados pela rede. Algumas ações estão citadas a baixo:

- Podem ser configurados diversos filtros no software, para que todas as requisições de conteúdo realizadas ao *Proxy* reverso sejam analisadas, a fim de garantir que nenhum conteúdo malicioso está em transmissão. Filtros esses que com assinaturas especificas indicam quais ações dever ser tomadas em caso de acessos indevidos.
- O armazenamento de logs de acessos, conteúdos acessados e transmitidos, são informações essenciais para que seja analisado pelo administrador, pois com

esse método, o *Proxy* reverso intercepta toda comunicação que passa por ele e realiza o armazenamento do conteúdo que se faz importância, como por exemplo, data e hora do acesso, conteúdo acessado, certificado IP. Tais informações são imprescindíveis para identificação de incidentes.

- O controle das informações de resposta pelo *Proxy* reverso é uma estratégia muito válida, pois ao deixar que uma mensagem de erro do *web server* interno seja transmitida direto ao host requisitante, é um risco a segurança do serviço, pois pode ser revelada informações estratégicas da topologia de rede interna da organização, tais como IPs, topologia e posicionamento do servidor na rede. Desta forma, uma função do servidor *Proxy*, é personalizar qualquer mensagem de erro de resposta do *web server* interno ao requisitante, fazendo com que desta forma a mensagem a ser transmitida, além de ser mais clara, não oferece riscos ao negócio.

3.4 Vantagens no uso do *Proxy* Reverso

A tecnologia ou filosofia do *Proxy* reverso oferece em seu uso, diversos benefícios para segurança, disponibilidade e desempenho no acesso aos serviços requisitados. Além de todas as vantagens de um *Proxy* comum citadas no capítulo 2.3, abaixo se encontram disponíveis outras de suas vantagens:

1) Devido ao fato do *Proxy* reverso ser a única interface externa da rede e ser isolado dos servidores, as identidades dos *web server*s não são conhecidas, assegurando que a requisição não sabe para onde seguirá;

2) A criptografia *SSL* pode ser delegada ao próprio servidor *proxy*, ao invés dos servidores *Web*. Neste caso, o servidor *proxy* pode ser dotado de aceleradores criptográficos de alta performance, pois s páginas que requerem acesso com criptografia SSL, ou também HTTPS consomem muito do processamento do servidor *Web*. Com o *Proxy* reverso, a criptografia é feita até este servidor envie uma requisição HTTP comum ao servidor *Web*, diminuindo o consumo de processamento;

3) O proxy reverso é inteligente o suficiente para fazer o Balanceamento de Carga. No cenário em que existem diversos web servers rodando com a mesma aplicação desejando distribuir as requisições para o servidor web que não está ocupado, o proxy reverso fica responsável por essa delegação. Ou seja, uma requisição chega ao Proxy Reverso, que por sua vez realiza o endereçamento para o servidor que está menos ocupado;

4) Caso o conteúdo requisitado seja estático ou passível de armazenamento, o *proxy* reverso pode responder de imediato com o conteúdo da requisição, evitando a consulta ao *web server* e contribuindo com a diminuição do processamento;

5) Facilidade em esconder o sistema operacional utilizado nos *web Server*s, dificultando que possíveis vulnerabilidades destes sistemas operacionais sejam exploradas;

6) Permite a utilização de uma base de autenticação como o *Active Directory* no Microsoft Windows ou um *RADIUS* (*Remote Authentication Dial-In User Service*) para que os acessos possam ser autenticados antes de repassar as requisições para o servidor *web* que hospeda o conteúdo requisitado. Esse mecanismo permite utilizar mais uma camada de segurança para aplicações que não foram projetadas seguindo um padrão mínimo de segurança, ou para aplicações antigas ou que trabalhem em um sistema que não forneça esse nível de proteção;

7) Permite que padrões de ataques conhecidos, como requisições HTTP que utilizam caracteres especiais *UNICODE* [21]sejam bloqueados diretamente no *Proxy* reverso;

8) A unificação de todos os logs de acessos no *Proxy* reverso facilita o gerenciamento do ambiente, a análise de trafego e o monitoramento da segurança.

As vantagens na utilização do *Proxy* reverso são muitas, como se pode observar. Se combinado com as configurações adicionais de segurança e técnicas de prevenção de riscos, pode garantir mais segurança ao principal ativo do negócio, a informação. (LOPES, 2006)

3.5 Desvantagens no uso do *proxy* reverso

A utilização do *Proxy* reverso trás alguns pontos de atenção que devem ser levados em consideração antes de sua implementação, como descritos abaixo:

- Qualquer alteração na aplicação que envolva URL ou subdiretórios deve ser replicada no *Proxy* reverso, caso contrário, o acesso a aplicação pode ficar indisponível;
- O conjunto de filtros e regras de bloqueios de padrões conhecidos de ataques devem ser revisados e planejados, pois poderá causar bloqueio do acesso de URL

[21] UNICODE - é um padrão que permite aos computadores representar e manipular, de forma consistente, texto de qualquer sistema de escrita existente.

permitidas. Todo este processo dependendo do numero de elementos configurados no *Proxy* reverso é um processo que pode consumir muito tempo dos administradores;

- Caso ocorra algum erro lógico na aplicação, ou seja, alguma falha no código da aplicação, a vulnerabilidade pode revelar dados do ambiente interno ou até mesmo acesso a outras bases de informações. Neste caso, a segurança deve ser aplicada e revisada no código da aplicação e não no *Proxy* reverso;
- A maquina onde o *Proxy* reverso é hospedado e executado dever ser de alta disponibilidade, pois como atua como ponto único de acesso ao *web server*, sua indisponibilidade afetará diretamente o acesso a aplicação e trará impacto ao negócio da empresa.(UILSON, 2011)

Ao optar pelo uso do *Proxy* reverso, todos estes pontos devem ser levados em consideração e utilizados para análise da tomada de decisões.

3.6 Algumas soluções que oferecem o *proxy* reverso

É possível encontrar no mercado diversas aplicações de *Proxy* que também realizam a função de *Proxy* reverso.

Conforme abaixo, segue as opções mais conhecidas e funcionais do mercado, onde é possível usufruir da função de *Proxy* reverso (LOPES, 2006):

- Apache (http://www.apache.org/);
- Cisco *Cache* Engine (http://www.cisco.com);
- Cisco CSM – Content Switch Module (http://www.cisco.com);
- Citrix NetCaler (http://www.citrix.com.br);
- F5 -Big IP (http://www.f5.com).
- ForeFront TMG 2010 (http://www.microsoft.com);
- ISA *Server* (http://www.microsoft.com);
- Nginx (http://wiki.nginx.org/);
- *Proxy*SG (http://www.bluecoat.com);
- Squid *Web Proxy Cache* (http://www.squid-*cache*.org);

Neste capítulo podemos observar as caracteristicas e conceitos do *proxy* reverso, sua utilização e como pode ser um aliado na segurança do acesso a servidores, atuando como uma camada a mais de segurança. Apresentamos vantagens e desvantagens em sua utilização, bem como dados a serem usados para tomada de decisão por sua utilização ou análise de possibilidades.

4. FERRAMENTA PARA CONFIGURAÇÃO DO PROXY REVERSO

4.1 **Apresentação da Ferramenta**

Busca continua da agilidade e produtividade são, e sempre serão, necessidades do negócio, porém contando com a proteção dos dados sensiveis de seus diversos meios de acessos.

A TI procura alinhar as necessidades do negócio com os desafios da segurança da informação, pois não basta somente disponibilizar acesso as plataformas de informações para tornar o negócio agil, é necessário uma solução que garanta o acesso de forma segura, confiável e íntegro, pensando também na reduçao de custos e na complexidade de implementação, administração e manutenção.

A ferramenta da Microsoft, o *Forefront Threat Management Gateway* (TMG), foi desenvolvida com base nos principais recursos do ISA *Server* para fornecer um gateway de segurança de rede integrado e abrangente, permitindo o uso dos recursos de rede de maneira produtiva e segura para o negócio, evitando transtornos com malwares e outras ameaças. Com o valor da licença empresarial aproximada de $75,000 (Setenta e Cinco Mil Dolares), o ForeFront TMG 2010 possui várias camadas de proteção, algumas são atualizadas continuamente pela Microsoft, como é o caso da filtragem de URLs, inspeção de malware, prevenção contra intrusões, *firewall* da camada de aplicativos e de rede e inspeção de HTTP/HTTPS, que são integradas em um gateway unificado, fácil de gerenciar, que reduz os custos e a complexidade da segurança da Internet.

A solução Forefront TMG inclui dois componentes:

1º) Forefront Threat Management Gateway 2010 *Server*: Fornece filtragem de URL, inspeção antimalware, prevenção de intrusão, *firewall* na camada de aplicativos e de rede e inspeção de HTTP/HTTPS em uma única solução;

2º) Forefront Threat Management Gateway Web Protection Service: Fornece atualizações contínuas de filtragem de malware e acesso a tecnologias de filtragem de URL baseadas em nuvem agregadas de vários fornecedores de segurança da *Web* para proteção contra as ameaças recentes baseadas na *Web*. (MicroSoft, 2012)

Além do foco principal na segurança, o pontos forte do ForeFront TMG é a facilidade na administração, pois todos os mecanismos de segurança estão centralizados em um único console de gerenciamento.

4.2 Vantagens e Requisitos

O TMG tem a capacidade de proteger a infra estrutura de forma eficiente e sem complexidades em sua administração.

Como definido pela equipe responsável pela solução, o Forefront TMG (sucessor do ISA *Server* 2006), não se resume somente a serviços de *firewall*, *Proxy* e *cache*. Esta solução atua como um *secure web gateway* que oferece recursos que vão além do controle de acesso internet de uma organização.

Algumas características definidas como pilares do Forefront TMG:

- Proteção de acesso de fora para dentro;
- Proteção de acesso de dentro para fora;
- Proteção contra ameaças de rede

As caracteristicas citadas acima, resumem-se como sendo acesso a servidores de correio, servidores de aplicação, *VPN*[22] e outros recursos publicados, inspeção de Malware e HTTPs, além de filtro URL para controle de acessos a determinados sites e recursos que foram aperfeiçoados tais como IDS (Intrusion Detection System) [23]e inspeções de rede.

O controle de acesso a internet é um dos pontos críticos de uma corporação. O bloqueio de um determinado site não garante que o usuário não irá acessar outro de mesma categoria, mas que não conste na sua regra de bloqueio.

Baseado nesta necessidade, o serviço de URL *filtering* bloqueia determinadas categorias de site tais como, nudez, pornografia, games, pedofilia, etc.

Este é um serviço agregado ao Forefront TMG, e as informações de categorização de sites são colhidas da Microsoft *Reputation Services* (MRS), ou seja, serviço em nuvem. Porém, para uso deste serviço é necessário a compra da licença de URL *filtering*.(UILSON, 2010)

Atualmente, para utilizar uma solução de URL *Filtering*, será necessário a aquisição de mais equipamentos e softwares, o que gera um custo muito maior se comparado a implementação da mesma solução pelo Forefront TMG, mesmo pagando um valor adicional pelo *download* de informações atraves do MRS.

[22] Virtual Private Network - Rede Privada Virtual, é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a Internet.
[23] IDS - *Intrusion Detection System* - Ferramenta de detecção de intrusão

Outro valor agregado nestes pilares principais da solução é a inspeção HTTPs, protocolo que procura garantir a segurança no tráfego de informações e transações comerciais e bancárias. Entretanto, nos dias de hoje alguns sites, mesmo em HTTPs, trazem ameaças a infra estrutura e o Forefront TMG, com o serviço de HTTPs *Inspection* protege fornece proteção a rede contra essas ameaças.

O TMG oferece recursos de inspeção de redes e *IDS*, que protegem a rede de vulnerabilidades Microsoft, evitando que possam ser exploradas, possibilitando realizar atualizações de segurança necessárias no ambiente.

Com a Integração com o *Active Directory*, o TMG simplifica a autenticação e a imposição de políticas integrando-se ao *Active Directory*. Por exemplo, o Forefront TMG 2010 simplifica a inspeção de HTTPS distribuindo seu certificado via *Active Directory*. Também usa a infraestrutura do Windows Update para permitir a rápida distribuição de novas proteções para todos os servidores Forefront TMG 2010.

> *"É necessária uma sintonia entre a área de TI e as demais áreas do negócio em várias vertentes, tais como:*
>
> - *A corporação precisa proteger dados importantes e seus pontos de distribuição. A área de TI precisa prover acesso seguro e fácil ao mais diversos tipos de dispositivos;*
> - *Para a continuidade dos negócios, a corporação precisa garantir acesso a seus colaboradores de qualquer lugar;*
> - *A corporação luta para diminuir custos com gerenciamento de recursos de segurança e a área de TI tenta diminuir a complexidade neste gerenciamento.*
>
> *Para todos esses pontos, o Forefront Threat Management Gateway, ou simplesmente TMG, é a solução que aborda diversas questões de segurança e mantém a produtividade da corporação."* (UILSON, 2012)

Para construção de uma solução semelhante, seria necessário um alto investimento em softwares, equipamentos, podendo gerar custos elevados para manutenção e administraçã o dos mesmos. O Forefront TMG oferece estes serviços, com redução de complexidade na manutenção e administração, além de um custo reduzido. (UILSON, 2012)

Existem pontos de atenção do ForeFront TMG que devem ser levados em consideração ao optar por esta ferramenta, sendo eles:

- Instalação do TMG em um controlador de domínio não é suportado;
- TMG roda somente em ambientes x64.

O ForeFront TMG necessita de um ambiente apropriado para instalação e configuração e exige alguns cuidados. O Forefront TMG 2010 requer um servidor com processador de 64 bits com dois núcleos de processamento, 2GB de RAM, 2.5 GB de espaço disponível no disco rígido, uma placa de Interface de rede compatível e uma partição de disco rígido local formatada em NTFS. Suporta Windows *Server* ® 2008 SP2 ou Windows *Server* 2008 R2. (MicroSoft, 2012).

4.3 *Proxy* Reverso com ForeFront TMG

Para a publicação de uma aplicação ou portal utilizando o ForeFront TMG no papel de *proxy* reverso, se faz necessário o seguinte cenário:

- O servidor do TMG deverá ter duas placas de redes (uma para rede interna e outra para rede externa);
- Certificado Digital emitido por uma entidade certificadora (CA) ou gerado internamente, caso a empresa seja habilitada;
- Um controlador de dominio associado ao ForeFront TMG.

Levando em consideração o ambiente acima e os dezenove passos de configurações que constam no anexo um deste trabalho garantem a publicação da aplicação de modo seguro utilizando o protocolo HTTPS e Autenticação através do *Active Directory*. (Technet Microsoft, 2012)

A Figura 7 exemplifica como o ambiente ficará após a configuração:

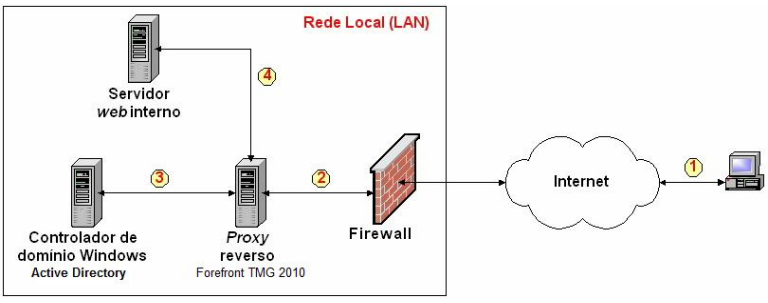


Figura 7. Topologia de configuração do *proxy* reverso (LOPES, 2006)

Por ser uma ferramenta baseada em um ambiente de sucesso, ISA 2006, o ForeFront desempenha com maturidade, simplicidade e com efetividade o papel de Proxy reverso, tornando-se uma camada bem consistente de segurança. Este tópico será abrangido no capítulo cinco deste trabalho.

5. ESTUDO DE CASO

Como podemos verificar, a importância na disponibilização de informações e mobilidade do acesso é cada vez mais necessária para tornar o negócio mais competitivo.

5.1 Exposição do cenário

A empresa AssineTV[24], utiliza um sistema ERP que gerencia toda base de clientes, ou seja, assinantes do principal produto da empresa, assinatura de TV via satélite.

Este sistema é dividido em interfaces diferentes para finalidades distintas, neste caso, para análise do problema, abordar-se-á somente a principal interface deste sistema ERP, que é a interface de vendas *WEB* chamada Vvendas.

O sistema VVENDAS é a principal ferramenta de vendas da AssineTV, onde é possível a contratação de produtos como pacotes de canais, assinatura de TV via satélite, Payper view entre outros. Seu acesso é restrito, disponível somente para rede interna da Empresa. Porém, o maior volume de vendas da empresa vem de parceiros credenciados, espalhados por todo território nacional.

5.2 Problema

A melhoria continua deve ser uma meta para toda empresa que queira não só ganhar um nome no mercado, como se manter ativa nele. Por este motivo, uma análise voltada para a melhoria do processo de venda da empresa foi iniciada.

Como informado, o maior volume de vendas da empresa origina-se de parceiros credenciados, porém desde o processo de inicio da venda com o parceiro credenciado até a conclusão do processo na empresa, pode-se dar margem para erro, desistência e possibilidade para concorrência ganhar o cliente.

O processo seguia da seguinte forma: A credenciada[25] realizava a venda através de um formulário impresso com todos os dados do cliente e ao final do dia, passava estas informações para empresa através de email, telefone, ou fax. Além da morosidade do processo, e as análises indispensáveis para venda, a validação de crédito e análise de CPF não eram realizada no momento da venda, ocasionando possíveis cancelamentos e transtornos.

[24] AssineTV – Nome fictício para preservação da marca da empresa
[25] Credenciada – Loja autorizada a utilizar o nome de uma franquia e vender produtos da mesma.

5.3 Primeira Tentativa de Solução

Após estudo de viabilidade da equipe de segurança da informação, a AssineTV decidiu por disponibilizar seu sistema de vendas na internet para que fosse possível agilizar o processo de vendas, melhorando o tempo de instalação do produto para o cliente e reduzindo em mais de 90% problemas de análise de créditos, uma vez que o resultado é imediato no momento do cadastro ao sistema.

Analisando a questão de possibilidades, foi pego como exemplo uma empresa também do ramo de assinatura de serviços a cabo, que por estratégia, utiliza exatamente o mesmo sistema de vendas que a AssineTV, porém com nome diferente, configurado ao seu negócio, sendo ela a COMPRETV[26].

A COMPRETV se deparou com o mesmo problema no atraso de suas vendas e também se decidiu em disponibilizar seu sistema para acesso externo, ou seja, na internet. Porém, optou por disponibilizar diretamente na internet, sem uso de uma barreira a mais de segurança, como por exemplo, uma autenticação extra.

Esta "vulnerabilidade" é um ponto de atenção imenso para a continuidade do negócio, pois uma vez que ocorra uma invasão ao sistema, é possível ter acesso a todo tipo de informações sigilosas da empresa, como por exemplo, dados pessoais de toda a base de assinantes, sendo possível inclusive, a extração destas informações para uso tendencioso e malicioso.

Pensando nisto, a AssineTV optou por utilizar uma barreira a mais na segurança de seu acesso, implementando assim uma ferramenta da empresa Check Point chamada Connectra, atuando como *Proxy* reverso.

Na floresta de domínios da empresa, foi criado um domínio adicional chamado externo.atv.br especificamente para os usuários que terão de realizar o acesso externo na ferramenta VVENDAS.

5.4 Ambiente de acesso

Para que um usuário possa realizar o acesso, a principal ferramenta de vendas da empresa além do *login*[27] e senha da ferramenta, o mesmo necessita ter um usuário criado no domínio externo.atv.br.

[26] CompreTv – Nome fictício para preservação da marca da empresa
[27] Login – Usuário, credencial de identificação que permite e identifica um usuário de sistema

5.5 Problemas no Acesso

A utilização da ferramenta Connectra gerou uma serie de problemas no acesso externo. Por ser um pouco limitada e com suporte descontinuado, a sua adequação ao negócio da empresa era praticamente nula se tornando um ponto questionável ao negócio.

Como não existia integração completa da ferramenta com o servidor de domínio *Active Directory*, a dificuldade na administração do acesso externo dos parceiros credenciados estava demandando muita mão de obra da equipe de *service desk*[28] da empresa, pois apresentava as seguintes deficiências:

- O usuário não conseguia alterar sua própria senha e nem recuperá-la em caso de perda;
- A definição de validade da do *Active Directory* não era valida para o Connectra, portando, uma vez que a senha expirava dentro de 60 dias, o acesso simplesmente era bloqueado, pois não existia possibilidade de troca da senha sem o contato com o Service Desk da empresa;
- A ferramenta Connectra não dava suporte a realização de *web cache*, portanto a lentidão no acesso era constante;
- O idioma de todos os menus era em inglês e por ser uma ferramenta que foi descontinuada, não havia possibilidade de alteração.

Como consequência destes diversos problemas, o impacto gerado diretamente no resultado financeiro da empresa e no Service Desk, foi necessário que a estratégia fosse alterada.

5.6 Solução definitiva encontrada

Após muita pesquisa e testes, mesmo com a pressão da área de negócios da empresa, a equipe de infra estrutura e segurança da informação optou por migrar o acesso do sistema VVENDAS para a ferramenta da Microsoft Fore Front TMG.

O TMG, como conhecido no meio tecnológico, é totalmente compatível com servidor de domínios *Active Directory*, contando ainda com pacote de idiomas em português. Possui função de *Web Cache* e balanceamento de carga tornando o acesso mais rápido.

Sua implementação foi realizada com a migração dos usuários em quatro ondas, uma a cada domingo do mês.

[28] Service Desk – Cicada no ITIL como ponto único de contato de uma empresa ou organização

5.7 Resultado

Foi possível perceber o resultado da mudança estratégica logo no primeiro mês, onde o resultado financeiro da empresa teve um aumento de 15% em relação ao mês anterior.

A integração total do AD com o TMG possibilitou que o usuário pudesse realizar a troca de sua senha e alteração em casos de senha expirada, reflexo percebido no volume de interações recebidas no mês pelo *service desk*, ocasionando uma queda de aproximadamente 50% no primeiro mês.

Chamados como lentidões no acesso também tiveram queda significante, de 53,5%, em função da utilização do *web cache* da ferramenta e balanceamento de carga.

A rápida mudança na estratégia seguida do envolvimento das áreas impactadas do negócio e com uma ferramenta funcional e personalizável, foi de suma importância para o sucesso do projeto e melhoramento dos resultados da empresa.

A partir do estudo de caso, foi possível ter uma visão mais ampla das necessidades do negócio e dos impactos causados por um ambiente mal configurado. A falta de planejamento e de comunicação dos todas as áreas envolvidas, impacta diretamente no resultado da empresa, perceptível também nos diversos departamentos, como por exemplo, *help desk*, comercial e administrativo.

Uma definição que dever ser tida como meta é o equilíbrio entre um ambiente muito fechado e um ambiente muito aberto, onde os impactos também foram exemplificados no estudo de caso. Para isto, a ferramenta ForeFront TMG 2010 atendeu de forma satisfatória as necessidades e requisitos do ambiente necessário para garantir a disponibilidade e segurança da aplicação e suporte ao negócio.

A Figura 8 ilustra a melhoria do entendimento dos fatores abordados para configuração do ambiente. (RITTA, 2008)

6. CONCLUSÃO

Disponibilidade, segurança, integridade e confiabilidade são palavras e termos chave para um ambiente organizacional ideal. A cada dia surgem mais empresas, mais empreendedores independentes, mais profissionais qualificados e estas palavras sempre são idealizadas como parâmetro a ser alcançado.

A correta utilização da mão de obra qualificada aliada a tecnologia existente no mercado e parâmetros idealizados pelo negócio, devem ser o ponto de partida para o planejamento das ações, no que se refere a segurança da informação na infra estrutura da organização.

Com este trabalho, foi possível analisar os pontos de atenção do negócio e as possibilidades de melhorias no ambiente interno e externo empresarial, que, se alinhado aos demais parâmetros e técnicas citadas nos cincos capítulos e levando em consideração a importância de um dos principais ativos do negócio - a informação - pode ser criado um ambiente não perfeito, porém bem controlado e mais próximo do ideal.

Foi possível analisar os impactos causados no negócio em caso de falha na disponibilização da informação, ou impossibilidade de acesso em ambiente muito seguro (fechado). O equilíbrio entre a segurança e disponibilidade é necessário para garantir que não haja impactos no negócio, atendimento e operacional.

De acordo com os pontos prós e contras da tecnologia do *Proxy reverso*, a ferramenta ForeFront TMG da Microsoft, entre as diversas semelhantes no mercado, se apresenta como uma opção funcional, de fácil administração e grande benefício para a segurança da informação corporativa, provendo uma camada significativa de segurança ao ambiente de TI.

REFERÊNCIAS

ABRANS, M., C.R.STANDRIDGE, ALBDULLA, G. WILLIANS, S. E FOX, E. [1995], 'Caching proxies: Limitations and potentials', in Proc. 4th Int. World Wide Web Conference pp. 119-133.

ABREU, D. Melhores Práticas para Classificar as Informações. Módulo e-Security Magazine. São Paulo, agosto 2001. Acesso em: Setembro 2012.

ANTONIO, J. Informática: questões da ESAF com gabarito comentado, Elsevier, 2007.

BRAGA, A. A Gestão da Informação. Disponível em: <http://www.ipv.pt/millenium/19_arq1.htm, 1996>. Acesso em: Setembro de 2012

CASSETTARI, H. H. Análise da Localidade de Programas e Desenvolvimento de Algoritmos Adaptativos para Substituição de Páginas. Qualificação de Mestrado. Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais. 2003.

CERT. Vulnerabilities, incidents & fixes, 2006. Disponível em: <http://www.cert.org/nav/index_red.html>. Acesso em: Outubro 2012.

DAWEL, GEORGE. A segurança da informação nas empresas - Ampliando horizontes além da tecnologia, Ciência moderna, 2005

ELIZABETH D. ZWICKY, SIMON COOPER & D. BRENT CHAPMAN, Building Internet Firewalls, 2000, Second Edition

FONTES, EDISON. PRATICANDO A SEGURANÇA DA INFORMAÇÃO. Ed. BRASPORT, 2008

GIBB, F.; BUCHANAN, S. A framework for business continuity management. International Journal of Information Management, Vol 26, Abril 2006

GURGEL, GIOVANE. O valor estratégico da informação para a gestão das organizações. XIII SIMEP, Baruru, 2006. Disponível em: <http://www.simpep.feb.unesp.br/anais/anais_13/artigos/967.pdf>. Acesso em Outubro de 2012

ICON S. Servidor Proxy e *cache*. Disponível em: <http://www.iconinfo.com.br/novo/servicos.php> Acesso em: Agosto 2012

IMMAGINARIO, R. Publicando um Servidor com o Forefront TMG. Disponível em: <http://technet.microsoft.com/pt-br/forefront/hh285684>. Acesso em: Setembro 2012

IT, WAY. PROXY. Disponível em: <http://www.movewayit.com.br/infraway.html> Acesso em: Setembro 2012

LOPES, LEANDRO S. SEGURANÇA EM SERVIDORES WEB UTILIZANDO PROXY REVERSO. Disponível em: <http://www.si.lopesgazzani.com.br/>. Acesso em: Agosto 2012

MALPANI, R., LORCH, K. E BERGER, D. [1995], 'Marking World Wide Caching servers cooperate', in Proc. 4Th int, World wide Web conference PP. 107-110

MAZIERO, C. 2010 - Algoritmos de substituição de páginas. <http://dainf.ct.utfpr.edu.br/~maziero/doku.php/so:algoritmos_de_substituicao_de_páginas> Acesso em Outubro de 2012

MICHAEL A. GALLO,WILLIAM M. HANCOCK, Padrões de arquitetura de aplicações corporativas, ARTMED EDITORA S.A, 2003

NBR ISO/IEC-17799 - Norma de Segurança da Informação

PONTES E, HIRATA S, HONORIO S. SEGURANÇA E ACELERAÇÃO DE INTERNET: UTILIZAÇÃO DE PROXY SERVERS PARA MANUTENÇÃO DE WEB *CACHE*S. Disponível em: <http://www.pontes.inf.br/docs/proxy.pdf>. Acesso em: Outubro 2012

RICHARD E. POTTER EFRAIM TURBAN R. KELLY RAINER, JR. ADMINISTRAÇÃO DE TECNOLOGIA DA INFORMAÇÃO. 2005, ELSEVIER

SANTANA, F. Introdução ao Forefront. Disponível em: <http://www.juliobattisti.com.br/fabiano/artigos/introducao_forefront.asp>. Acesso em: Setembro 2012.

SILVA D. O. Proxy reverso com Apache + *cache* + compactação + estatísticas. Disponível em: <http://img.vivaolinux.com.br/imagens/artigos/comunidade/proxy.gif> Acesso em Agosto 2012

SOLUÇOES P. O que é um servidor *Proxy*. Disponível em: <http://www.projetasolucoes.com.br/archives/804> Acesso em: Agosto 2012

SOUZA, UILSON, Tmg Reporter. Disponível em: http://uilson76.wordpress.com. Acesso em: Setembro 2012

STAREC, C.; GOMES, E.; BEZERRA, J. Gestão estratégica da informação e inteligência competitiva. 1 ed. São Paulo: Editora Saraiva, 2005.

TANENBAUM, A. S. Redes de computadores. 4ª Ed. Rio de Janeiro, Brasil: Ed. Campus, 2003.

TECWAN. Proxy. Disponível em: <http://www.techwan.com.br/solucoes/proxy.html>. Acesso em Setembro 2012

THE INTERNET SOCIETY. RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1.

TORRES, N. A.. Competitividade empresarial com a tecnologia da informação. São Paulo : Makron, 1994.

United States, 1999.[176]p. Disponível em: http://www.faqs.org/rfcs/rfc2616.html.

Tradução disponível em: <http://www.nacaolivre.com.br/open-source/traducao-rfc-2616/> Acesso em: Setembro 2012.

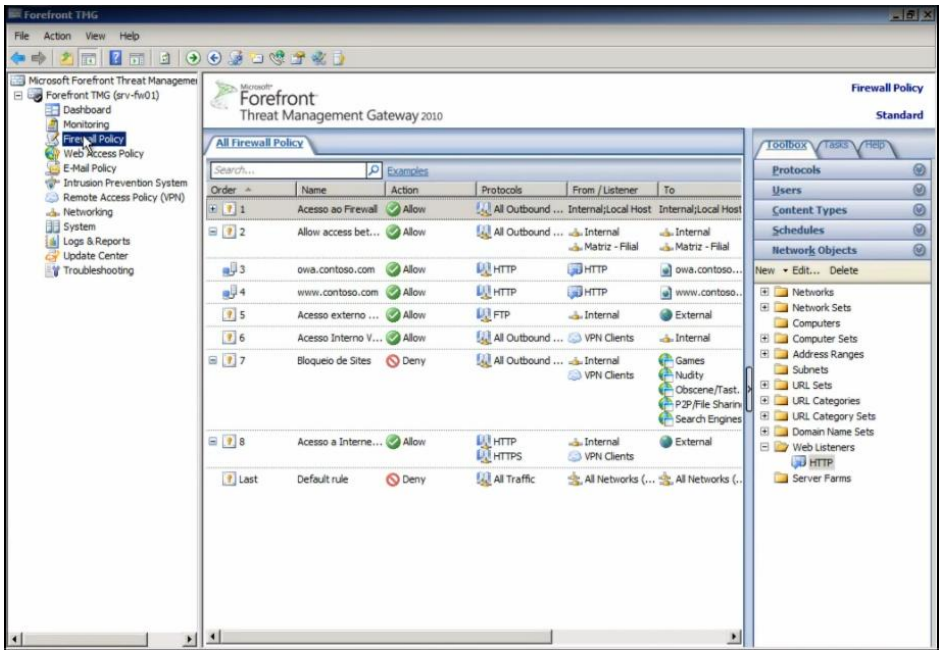
VELTEM, F. L. Publicação do Lync Server Reverse Proxy no ForeFront TMG 2010. Disponível em: <http://social.technet.microsoft.com/wiki/contents/articles/5195.publicacao-do-lync-server-reverse-proxy-no-forefront-tmg-2010-pt-br.aspx>. Acesso em: Setembro 2012

ZHOU J. Proxy and Reverse Proxy. Disponível em: <http://zhous.net/groups/basicnetworking/wiki/1f47a/images/59cac.jpg>. Acesso em: Agosto 2012

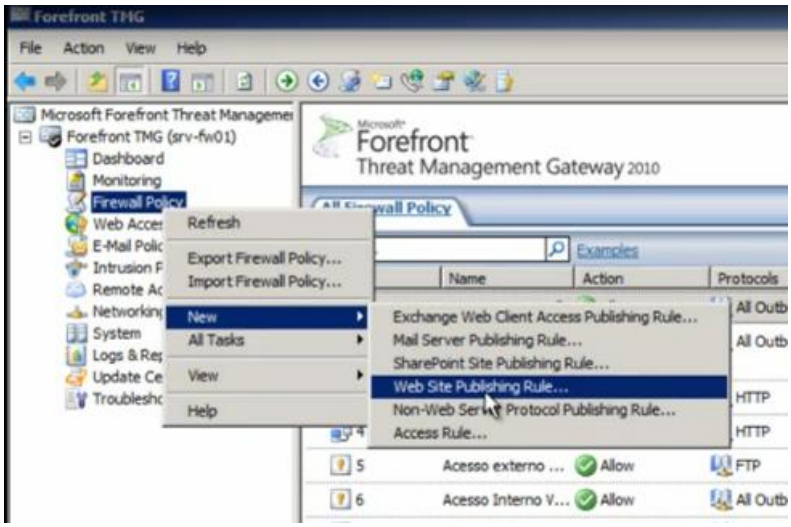
ANEXO 1 - Como publicar um portal ou aplicação de forma protegida utilizando o ForeFront TMG com Certificado Digital

Todas as figuras utilizadas neste tutorial são de *Print Screens* realizados do video "Instalando Certificado Digital no Forefront TMG com publicação de aplicação" disponível no link: http://technet.microsoft.com/pt-br/forefront/hh285683.

Passo 1 – Com o TMG aberto, clique com o botal direito do mouse no menu "Firewall Policy"

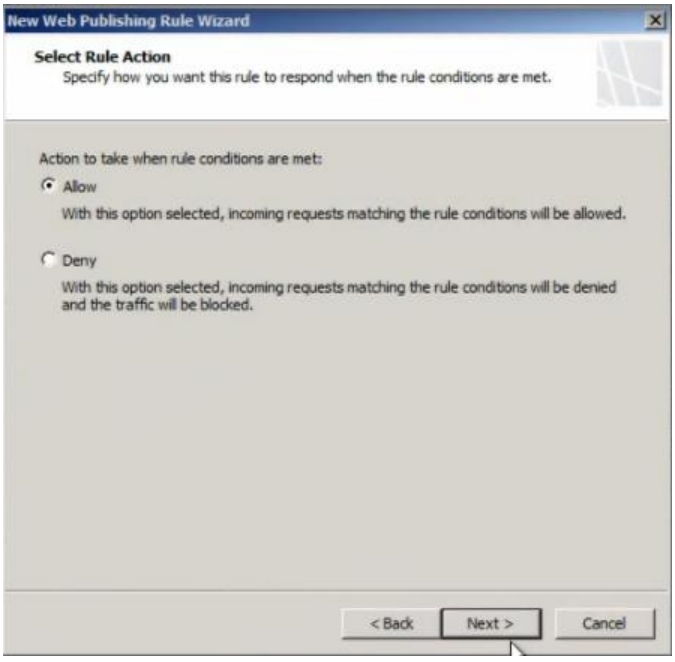


Passo 2 – Acesse a opção "New" e em seguida clique em "Web Site Publishing Rule"

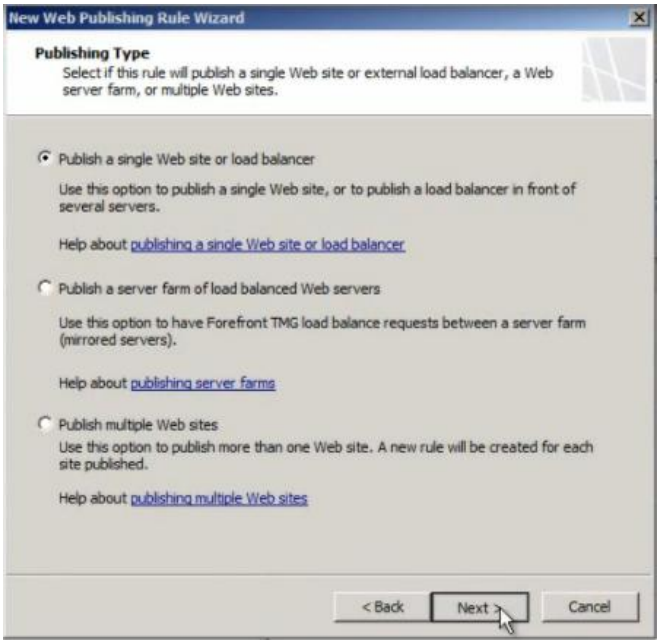


Passo 3 – Entre com o nome do site/portal a ser publicado e clique em “NEXT”

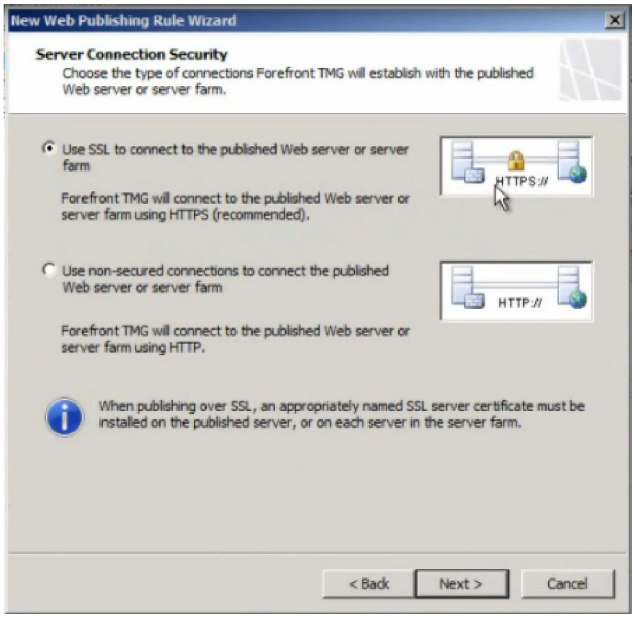
Passo 4 – Confirme que é uma regra de permissão (Allow) e clique em “NEXT”



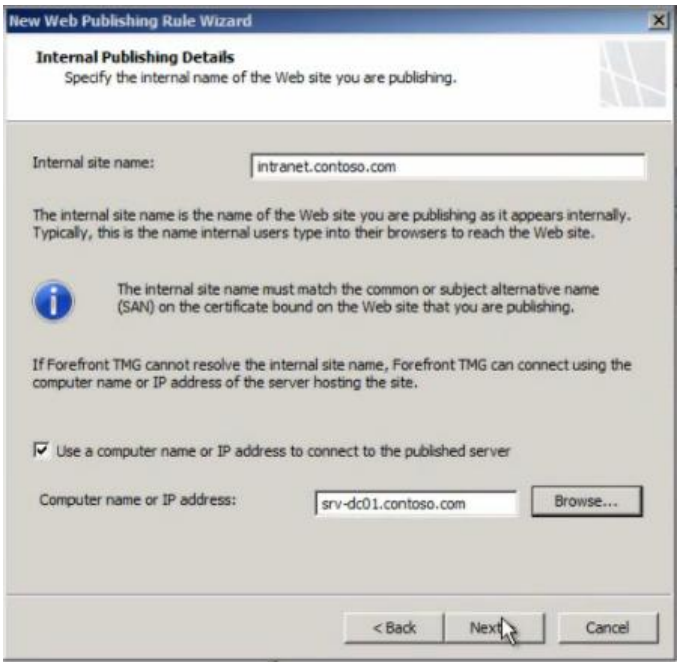
Passo 5 – Confirme a publicação de um único Site e clique em “NEXT”



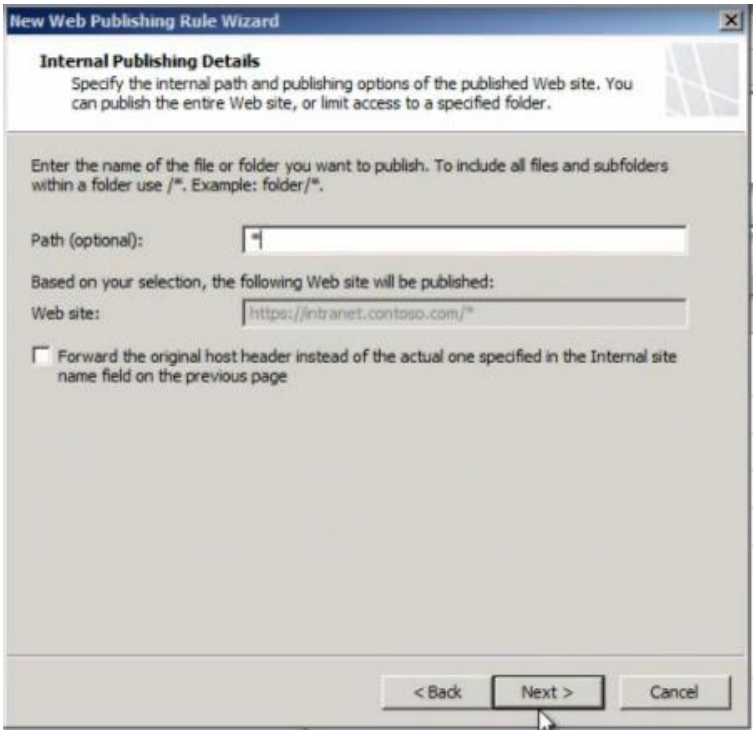
Passo 6 – Indique a utilização de SSL e Certificado Digital (HTTPS) e clique em “NEXT”.



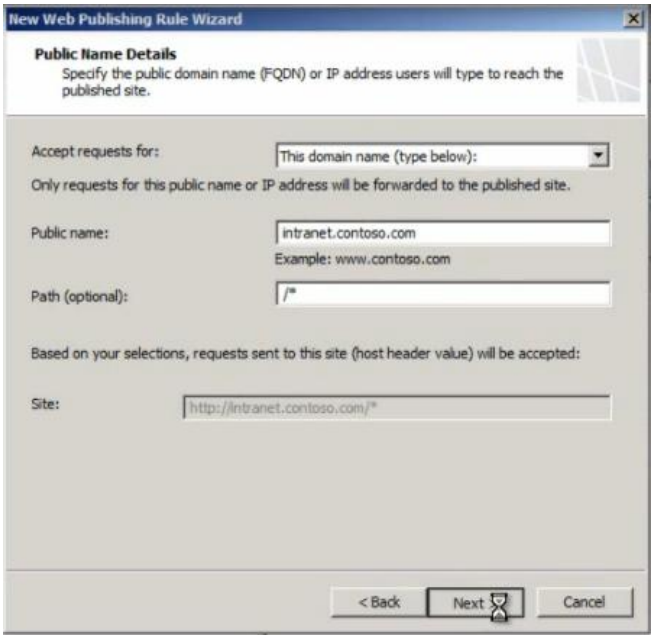
Passo 7 – Digite novamente o nome do site e localize o servidor de hospedagem no controlador de domínio, e clique em “NEXT”



Passo 8 – Informe os diretorios a serem publicados. Por padrão o TMG identifica os diretorios padrões. Adotaremos “*” para tudo seja publicado.

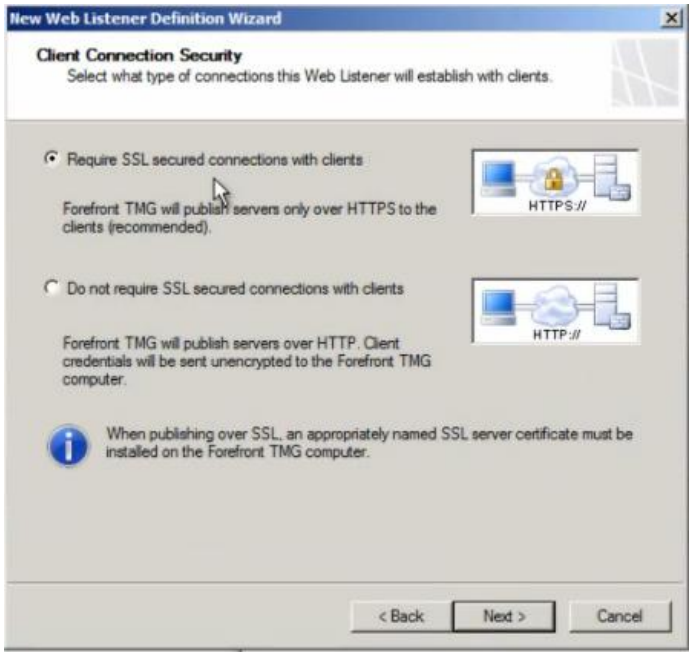


Passo 9 – Digite o nome desejado para publicação

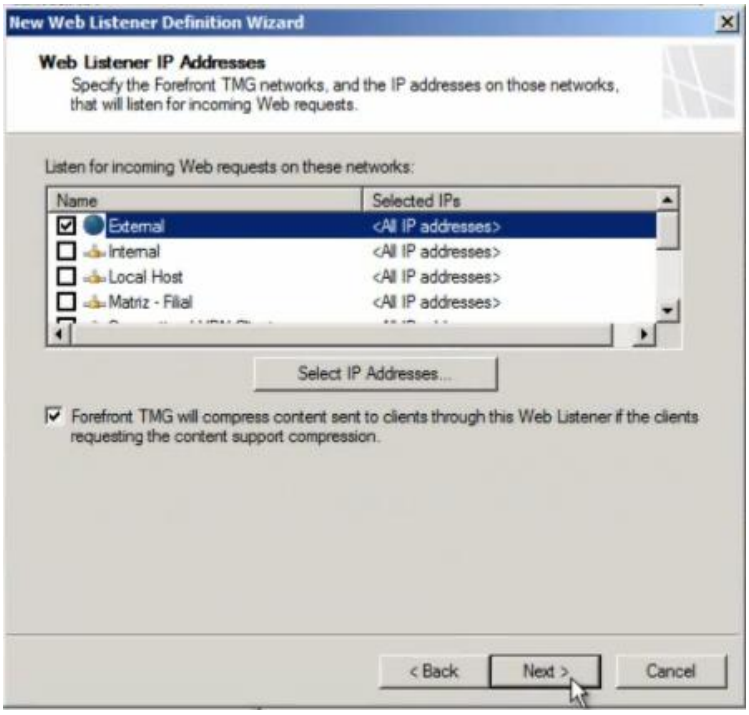


Passo 10 – Neste ponto, deve-se escolher a opção de publicação com protocolo HTTPS

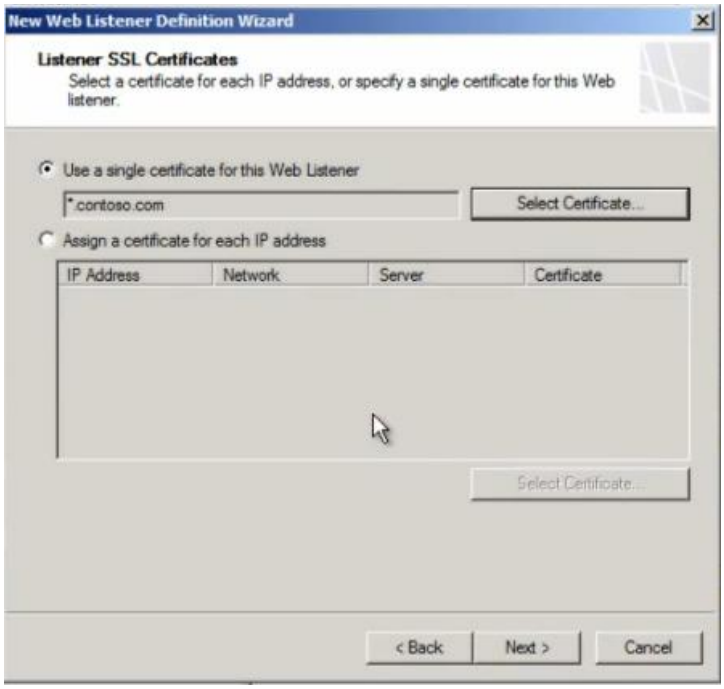
Passo 11 – Confirme a utilização de certificado digital conforme imagem abaixo



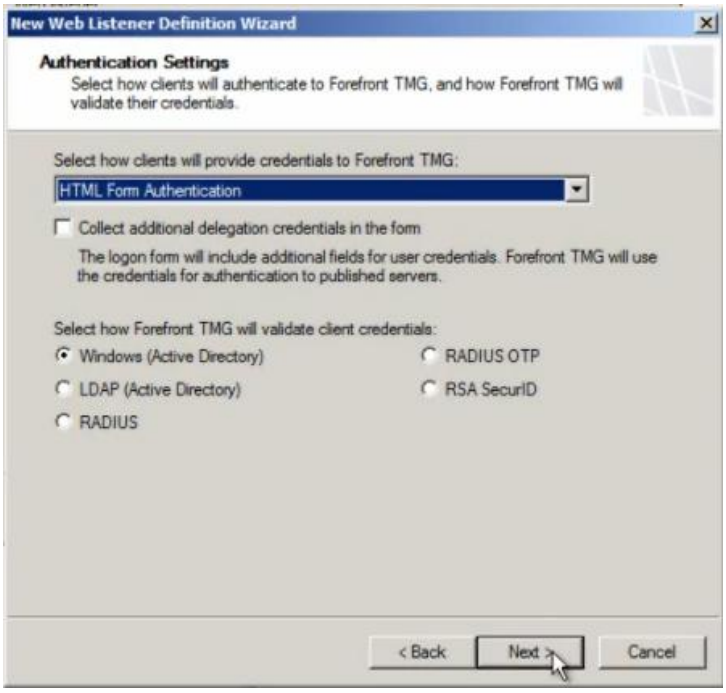
Passo 12 – Escolha a opção External, para indicar a utilização de certificado para acesso externo.



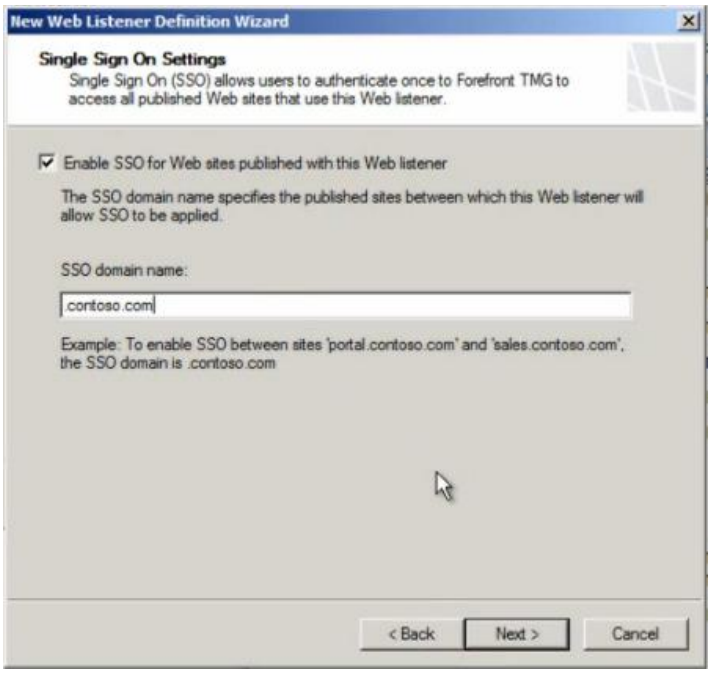
Passo 13 – Realize a importação do Certificado Digital



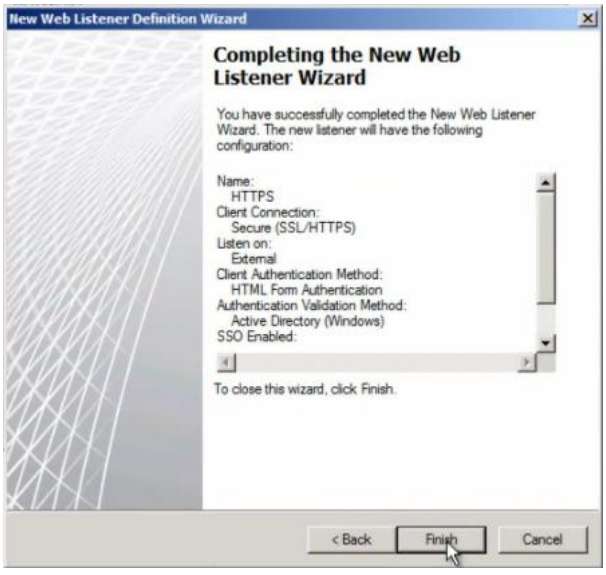
Passo 14 – Escolha a opção HTML Form Authentication, e indique a utilização do Windows (Active Directory) para autenticação.



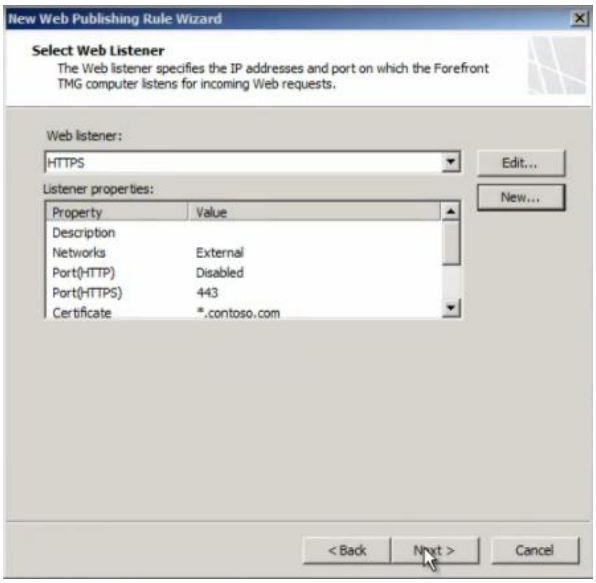
Passo 15 – A opção Single Sing On (SSO) indica que não será necessário se autenticar novamente em caso de acesso a mais de um diretorio para o dominio publicado (opcional).



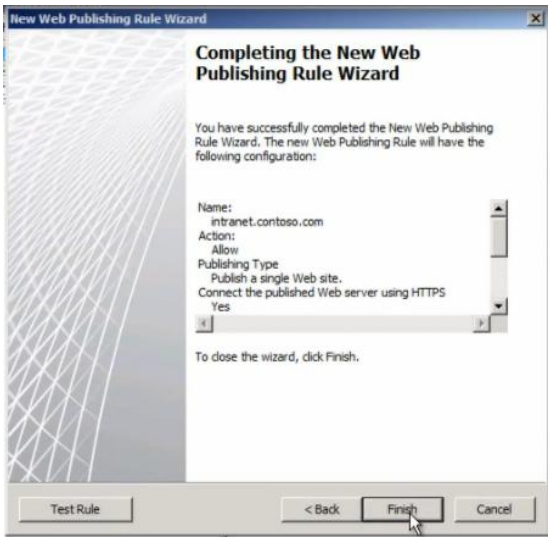
Passo 16 – A partir deste momento, será concluida a regra de publicação do site/portal/aplicação, exibindo o resumo das opções e configurações escolhidas.



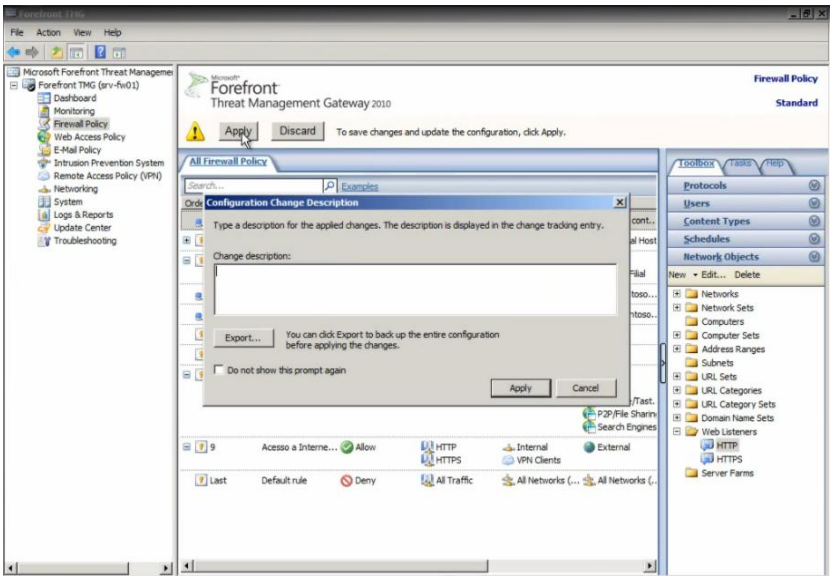
Passo 17 – Necessário confirmar a utilização do protocolo HTTPS



Passo 18 – Tela de confirmação da criação da regra



Passo 19 – Ao voltar para página principal do TMG, será exibida a mensagem conforme abaixo, informando a criação de uma nova regra e a opção de aplicar a regra.



Passo 20 – Como pode ser visto abaixo, a aplicação/site/portal, foi publicado com sucesso com autenticação no *Active Directory*.