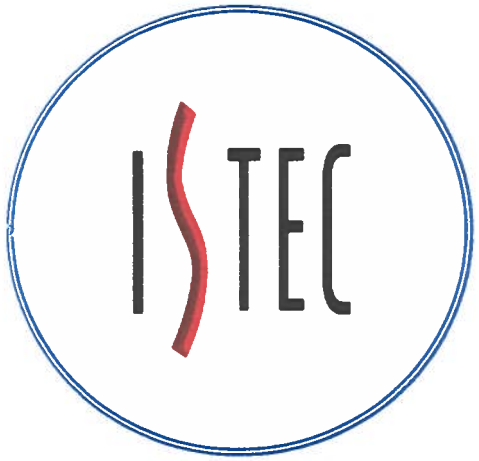

NETWORK ACCESS PROTECTION

Licenciatura em Informática

Ricardo Daniel Ferreira Pinto

Nº aluno: 1792

2014/2015

Lisboa

Orientador Metodológico: Professor Dr. Pedro Brandão

Este trabalho não se encontra escrito ao abrigo do novo acordo ortográfico.

Dedicatória

Dedico este trabalho à minha mulher Ariana e ao nosso filho Daniel por toda a força e coragem mostrada em seguir com este projecto. Ao Professor Dr. Pedro Brandão pela compreensão e ajuda no decurso deste projecto assim como os meus estimados colegas de curso, João Viera, Fábio Santos, Rafael Maya e Pedro Paixão.

Agradecimentos

Este projecto simboliza um marco no meu percurso académico, na minha vida pessoal e profissional, a licenciatura em informática. Este marco não me foi possível concluir com sucesso sem ajuda dos meus colegas e professores do Instituto de Tecnologias Avançadas de Lisboa.

Ao orientador do Projecto Global, Professor Dr. Pedro Brandão, pelo total apoio e disponibilidade que demonstrou desde o início da escolha do tema para este projecto como referência às aulas administradas na cadeira de Administração de Redes que foram essenciais para a elaboração deste projecto.

À Ariana pela motivação e coragem demonstrados assim como incentivo, carinho, compreensão e dedicação em todos os momentos.

Aos meus pais, pela vida que me proporcionaram e pelas regras de ética e morais que me incutiram, fazendo de mim a pessoa que sou hoje.

Aos meus amigos e colegas, pela amizade, ajuda e apoio incondicional que me deram na realização deste projecto.

A todos os professores com que tive oportunidade de aprender no ISTEC.

Resumo

Network Access Protection (NAP) é uma das mais antecipadas funcionalidades do sistema operativo Windows Server 2008. É uma nova plataforma que permite os administradores de redes especificar os níveis de acesso à rede. Tem como base a identidade do cliente, grupo onde está inserido e o grau de acesso determinado pela política implementada. Se um cliente não é compatível NAP disponibiliza um mecanismo automático para colocar o cliente em conformidade (um processo conhecido como remediação) e, posteriormente, aumenta de forma dinâmica o seu nível de acesso à rede.

NAP é uma plataforma extensa que fornece componentes de infra-estrutura e uma aplicação de interface programável (API) para adicionar componentes que verificam e corrigem a integridade do computador e força vários tipos de acesso de rede ou de comunicação.

Este projecto tem como objectivo dar a conhecer a funcionalidade NAP e compreender os benefícios da mesma para a organização onde é implementada, assim como, entender processos fundamentais do NAP para restringir e remediar o acesso do cliente.

Como componente prática do projecto demonstrarei o ambiente implementado em funcionamento com o recurso a DHCP, provocando alterações nas configurações de segurança do computador de modo a demonstrar o funcionamento desta funcionalidade.

Abstract

Network Access Protection (NAP) is one of the most anticipated features of the Windows Server 2008 operating system. NAP is a new platform that allows network administrators to specify levels of network access based on a client's identity, the groups to which the client belongs, and the degree to which the client complies with corporate governance policy. If a client is not compliant, NAP provides a mechanism for automatically bringing the client into compliance (a process known as remediation) and then dynamically increasing its level of network access.

NAP is an extensible platform that provides infrastructure components and an application programming interface (API) for adding components that verify and remediate a computer's health and enforce various types of network access or communication.

The main focus of this project is to introduce the NAP feature and understand the benefits for an organization which is implemented as well and understand fundamental NAP processes like client access restriction and remediation.

For the purpose of this project, I will demonstrate the deployed environment design with DHCP enforcement, causing changes in the computer's security settings in order to demonstrate the operation of this feature.

Abreviaturas

NAP – Network Access Protection

API – Application Programming Interface

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

RAM – Random Access Memory

GPO – Group Policy Object

NPS – Network Policy Server

IP – Internet Protocol

SHV – System Health Validator

SoH – Statement of Health

WSHV – Windows Security Health Validator

FTP – File Transfer Protocol

Índice Geral

Índice de Figuras

Índice de Tabelas

Capítulo 1 – Introdução

O conceito de segurança nas redes informáticas é fundamental para garantir o completo funcionamento das infra-estruturas de TI, a implementação foi evoluindo ao longo dos tempos mas sempre garantindo o seu conceito e objectivo.

Uma das implementações é um serviço de rede denominado de NAP, uma tecnologia de segurança do NPS da Microsoft que foi introduzida no Windows Server 2008. Inclui componentes que permitem criar e impor directivas de requisito de integridade que definem as configurações necessárias tanto de *software* como de sistema para os computadores que se conectam à rede.

NAP para além de proteger a rede tem como vantagem o facto de ser eficaz ao nível de custos e extensível:

Relativamente à protecção de rede, NAP fornece informações, ferramentas e métodos que ajudam a proteger a rede de riscos de segurança tais como:

- Análise de integridade do sistema: permite aos administradores de redes avaliar e monitorizar a integridade de um sistema numa organização em uma base contínua;
- Validação de políticas: verifica a eficácia das políticas de segurança existentes e permite a monitorização do efeito de novas políticas;
- Identificação de riscos: ao criar um perfil de verificação de integridade do sistema, NAP permite identificar e resolver possíveis riscos de segurança;
- Integridade da rede reforçada: melhora o estado de integridade da rede, restringindo o acesso a computadores que não estão em conformidade com as políticas impostas e trata de efectuar a remediação;
- Conformidade de políticas: fornece um mecanismo para verificar continuamente a conformidade com as políticas de integridade da rede;
- Controlo de acesso: fornece uma camada de segurança adicional, que permite tomar decisões políticas no momento de acesso à rede.

No que diz respeito à redução de custos e complexidade, NAP é rentável e menos complexo de implementar do que outras soluções, por ser um serviço integrado no próprio sistema operativo:

- Automatizar a aplicação de políticas: os clientes NAP recebem automaticamente o acesso completo ou restrito com base nas configurações definidas;
- Automatizar a remediação do cliente: os computadores que não estão em conformidade com as políticas de integridade da rede definidas podem ser automaticamente colocados em conformidade;
- Escalabilidade da infra-estrutura existente: ao fornecer uma escolha de métodos de imposição, o NAP pode integrar facilmente na infra-estrutura existente;
- Adicionar novos recursos facilmente: permite facilmente introduzir novos requisitos de integridade ou alterar o âmbito dos requisitos existentes.

Finalmente, NAP é uma solução extensível, baseada em padrões com muitos parceiros, fornecendo extensões à sua funcionalidade tais como:

- Padrões de tecnologia de escalabilidade: o protocolo SoH usado pelo NAP foi publicado como uma especificação da *Trusted Network Connect* (TNC), permite garantias de integração de operações através dos fornecedores das TI e as tecnologias de rede.
- Escolha de vários fornecedores: permite a integração do controlo de acesso entre vários fornecedores da área, como é o caso de segurança de clientes, gestão de actualizações, redes e sistemas de integração.

O objectivo deste projecto, além de comprovar os benefícios acima referidos, é demonstrar passo-a-passo como implementar num ambiente de laboratório a tecnologia NAP recorrendo ao DHCP para controlo de acesso da rede. Utilizando para tal a versão Windows Server 2008 R2, que contém instalado o DHCP e o NPS, e um cliente com o sistema operativo Windows 7 instalado, com o serviço de agente NAP ligado, assim como a componente de cliente de imposição do DHCP. Para que isto seja possível, é utilizado um controlador de domínio provido de servidor DNS.

Capítulo 2 – Estado de Arte

A utilização de computadores isolados representa um risco mais elevado de utilização, face aos implementados numa rede informática, seja ela isolada ou ligada a outras redes. Dado que os recursos existentes num dado computador ficam potencialmente ao alcance de vários utilizadores. (Hughes, 1995)

Sendo actualmente a utilização de sistemas em rede indispensável, é necessário adoptar mecanismos de segurança, suportados por tecnologias e ferramentas apropriadas, que garantem a protecção da informação e de outros recursos essenciais dos sistemas de informação. (Hughes, 1995)

A segurança de um sistema ou rede informática abrange diversos aspectos complementares, como por exemplo, autenticação de utilizadores e encriptação das comunicações, ligados por um conjunto diversificado de mecanismos de segurança. Esses mecanismos, que podem ser mais ou menos elevados, existem para fazer face a ameaças com diversas origens e/ou motivações. (Hughes, 1995)

Uma política de segurança é suportada pela determinação do nível de segurança, os custos de implementação e os seus benefícios. (Kizza, 2009)

O problema da segurança em sistemas e redes pode ser verificado através de vários aspectos distintos, sendo os mais revelantes os seguintes: autenticação, confidencialidade, integridade, controlo de acesso, "não repúdio" e disponibilidade. (Hughes, 1995)

1 – Conceitos Gerais

1.1 Autenticação

A autenticação é um dos aspectos fundamentais de segurança. É um procedimento através do qual é validada a identidade de um utilizador, dispositivo ou processo. Em muitos casos, antes de fazer sentido qualquer tipo de comunicação ou qualquer tipo de mecanismo para a garantia de outros aspectos de segurança, é necessário previamente garantir que as entidades intervenientes são quem afirmam ser. (Hughes, 1995)

1.2 Confidencialidade

A confidencialidade reúne as vertentes de segurança que limitam o acesso à informação, seja a utilizadores humanos, computadores ou sistemas. Existe um grande número de casos onde este aspecto é de extrema importância, no entanto, existem outros casos onde não existe necessidade nesta área. (Hughes, 1995)

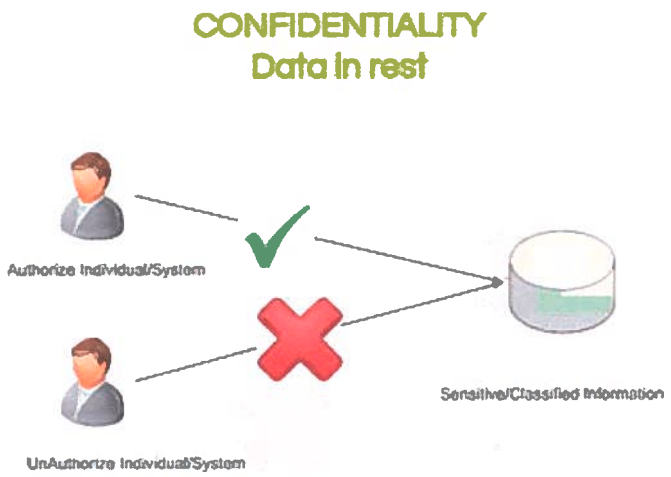

Figura 1 - Confidencialidade sem fluxo de informação (Certiology, 2014)

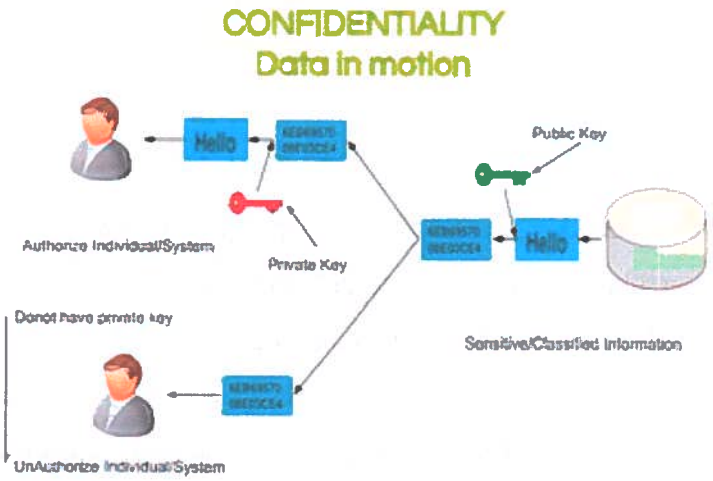

Figura 2 - Confidencialidade com fluxo de informação (Certiology, 2014)

1.3 Integridade

Na maior parte dos casos, para além de ser importante garantir a confidencialidade da informação que está a ser transmitida ou armazenada, é essencial que essa mesma informação não seja corrompida. Os aspectos de integridade abordam esse tipo de problemática da segurança. (Hughes, 1995)

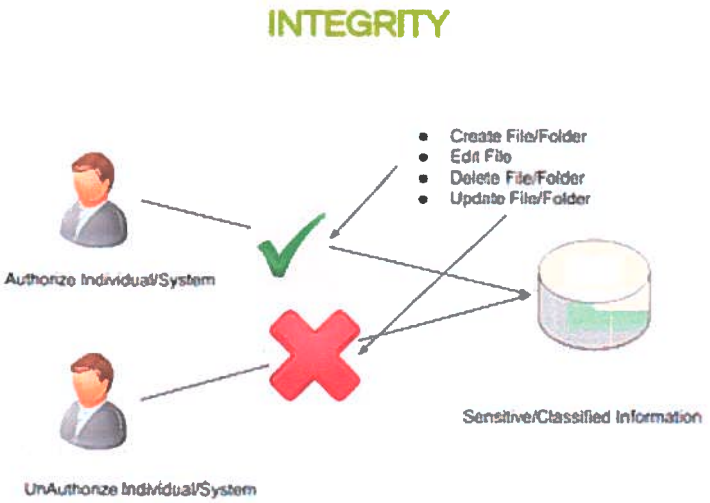

Figura 3 - Integridade (Certiology, 2014)

1.4 Controlo de acesso

A capacidade de impedir o acesso não autorizado a um recurso é genericamente designada por controlo de acesso. Por vezes, são incluídas na categoria de controlo de acesso as funções que limitam a quantidade de recursos a utilizar, o que é correcto de um ponto de vista de contabilização, mas não de um ponto de vista de segurança. Associados ao controlo de acesso, estão, normalmente, funções de autorização, que estabelecem os direitos de utilizadores, grupos e sistemas. (Hughes, 1995)

1.5 "Não repúdio"

Em muitas interacções, sobretudo em aplicações de comércio electrónico e aplicações bancárias, é de extrema importância que uma entidade envolvida numa transacção não possa negar a sua participação nesse evento. As funções que impedem que uma dada entidade negue a execução de determinada acção são designadas funções de não repúdio. (Kizza, 2009)

1.6 Disponibilidade

Os aspectos de disponibilidade garantem que, após a ocorrência de ataques a uma dada rede ou sistema informático, os recursos-chave ficam disponíveis para os utilizadores. Geralmente a disponibilidade não é garantida imediatamente, uma vez que é necessário, após um ataque, avaliar os danos causados e repor os sistemas num estado coerente. (Hughes, 1995)

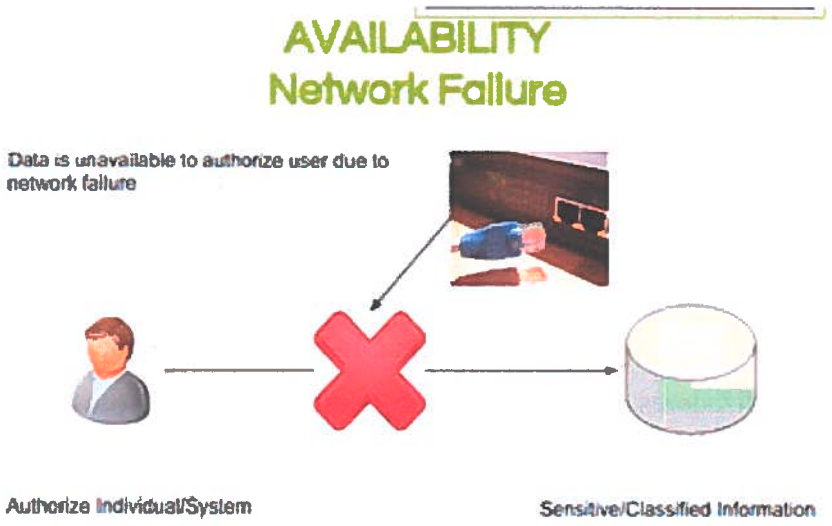

Figura 4 – Disponibilidade em falha de rede (Certiology, 2014)

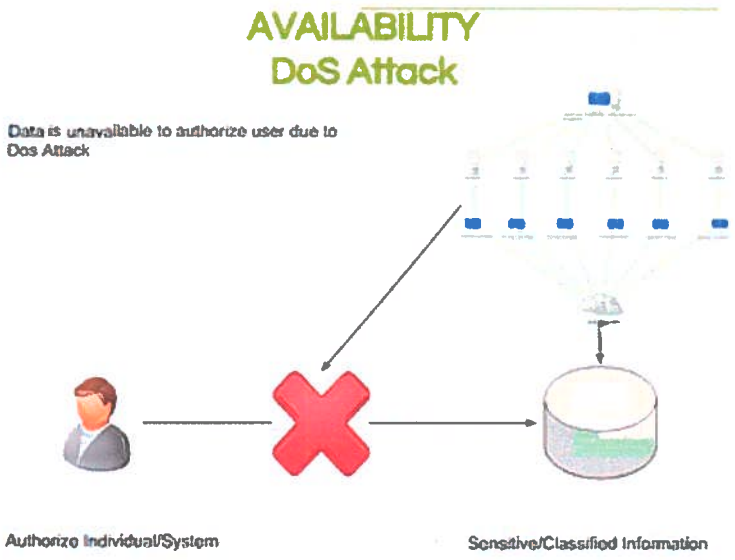

Figura 5 - Disponibilidade em ataque DoS (Certiology, 2014)

Os diversos aspectos de segurança acima referidos são, claramente, complementares, devendo a sua conjugação ser feita caso-a-caso, em função das necessidades de segurança específicas da rede que, por sua vez, são condicionadas pelos objectivos e natureza da organização que a detém. (Kizza, 2009)

2 – Conceitos Técnicos

2.1 *Server Roles*

Por ser um sistema modular, o mesmo pode ser configurado com componentes nas quais se destinam a validar contas de utilizadores, a partilhar ficheiros ou a desempenhar o papel de servidor de impressora. (Server Roles and Technologies in Windows Server 2012 R2 and Windows Server 2012, 2012)

2.2 Ferramentas Administrativas

As ferramentas administrativas ou *Administrative Tools*, são o conjunto de aplicações que permitem configurar e gerir os vários componentes do servidor. (Server Manager Step-by-Step Guide: Scenarios, 2008)

2.3 Gestão Centralizada

A administração de uma máquina pode ser feita de forma centralizada a partir de uma ferramenta chamada *Server Manager* ou Gestor de Servidor. (Server Manager, 2008)

2.4 *PowerShell*

A *PowerShell* é uma interface de linha de comando e uma linguagem de script, criada com o propósito de efectuar operações sem recurso à interface gráfica. (How Windows PowerShell Works, n.d.)

2.5 Aplicações *web*

Este componente opcional torna um servidor Windows numa plataforma segura, de fácil manutenção e de elevado desempenho para desenvolvimento e exploração de aplicações que ocorrem num *browser* como o Internet Explorer. (Internet Explorer, s.d.)

2.6 *Server Core*

Consiste numa variante da instalação normal, na qual é instalado apenas o núcleo do sistema operativo. A gestão é feita da linha de comandos ou mediante acesso remoto. Após a instalação, o sistema operativo pode ser configurado para desempenhar uma ou mais das seguintes funções:

- Servidor de virtualização;
- Servidor DHCP;
- Servidor DNS;
- Servidor de ficheiros;
- Servidor de *Active Directory*;
- Servidor de *Active Directory Lightweight Directory Services*;
- Servidor de *Active Directory Certificate Services*;
- Servidor de *Media*;
- Servidor de impressão;
- Servidor *Web* (IIS).

As grandes vantagens numa instalação deste tipo dizem respeito às áreas do desempenho, da segurança e da disponibilidade. Ao nível do desempenho, visto que os serviços instalados são mínimos e não existe interface gráfica, não ocorre grande carga, pelo menos inicial, sobre o servidor. (Ondrusek, 2010)

2.7 *Hyper-V*

O *Hyper-V* é a tecnologia de virtualização da Microsoft, é possível emular uma ou várias máquinas virtuais baseadas em *software*, nas quais é possível instalar sistemas operativos e outras aplicações como se estivéssemos a trabalhar com uma máquina real. (Hyper-V Getting Started Guide, n.d.)

2.8 Implementação de *Clusters*

Um *cluster* é uma implementação de redundância que consiste no agrupamento de vários grupos de computadores ligados entre si, vistos na rede como um único. Cada um dos computadores que constituem o *cluster* é denominado de "nó", sempre que um destes "nós" tem uma falha, outro assume as suas funções, garantindo um nível mínimo de paragens. (Natário, Alta disponibilidade - Terminologia (II), 2011)

2.9 *Network Load Balancing*

Network Load Balancing (NLB) é uma funcionalidade que permite a distribuição da carga das aplicações de clientes por múltiplos servidores, garantindo, assim, disponibilidade e desempenho elevados. Uma das utilizações típicas é em servidores *Web,* em que vários servidores garantem sempre tempos de resposta satisfatórios. (Natário, Balanceamento de Carga (V), 2011)

2.10 *Self-Healing New Techonology File System* (NFTS)

Possui um mecanismo que corre de forma transparente para o utilizador e faz verificações ao sistema de ficheiros automaticamente, procedendo às respectivas correcções sempre que seja detectado um problema. (Self-Healing NTFS, n.d.)

2.11 *Resilent File System*

O *Resilent File System* é o novo sistema de ficheiros do Windows Server 2012, que oferece uma robustez acrescida ao sistema de armazenamento. Embora forneça um aumento da integridade, disponibilidade, escalabilidade e pró-actividade na detecção de erros, não suporta algumas das características do NFTS. Nomeadamente, a compressão, encriptação ao nível dos ficheiros e quotas de discos. Também não é possível ser usado no volume de arranque de sistema. (Lucas, 2013)

2.12 Encriptação de discos *BitLocker*

Um dos grandes problemas da segurança de dados diz respeito à relativa facilidade com que alguém acede aos mesmos sem as devidas autorizações. Neste mecanismo de protecção, o disco rígido pode ser encriptado e os dados que nele contém só podem ser acedidos a partir do sistema operativo original. (Windows BitLocker™ Drive Encryption Step by Step Guide, s.d.)

2.13 Isolamento do servidor e do domínio

Quando existem grandes necessidades de segurança, podemos isolar quer um servidor quer um domínio do resto da rede, tornando-os inacessíveis do exterior, mesmo que toda a rede partilhe a mesma estrutura física.

Este isolamento pode ser feito de duas formas: isolando um servidor configurando políticas de *Internet Protocol Security* (IPSEC), de forma a permitir conexões a partir de determinados computadores clientes, ou isolando um domínio usando o *Active Directory* e garantindo que apenas são efectuadas conexões a partir de computadores membros desse domínio. (Network Policy and Access Services, n.d.)

O administrador pode ainda, usando uma característica chamada *Network Access Protection* (NAP), definir critérios ou requisitos de segurança que os clientes têm de cumprir rigorosamente para poderem usar os recursos de comunicação. (Network Policy and Access Services, n.d.)

2.14 *Read-Only Domain Controller* (RODC)

Suporte para uma configuração de controladores de domínio só de leitura, uma réplica do *Active Directory* com todas as funcionalidade comuns, tais como validar utilizadores, excepto a de criar novos objectos ou alterar os existentes.

Esta funcionalidade torna-se útil em instalações onde a parte da rede se encontra num local remoto, nas quais a segurança física é difícil de monitorizar ou garantir. (What Is an RODC, 2012)

2.15 *Firewall* do Windows com segurança avançada

A *firewall* do Windows permite o bloqueio de tráfego protegendo-o de utilizadores e aplicações com intenções duvidosas.

A sua configuração pode ir ao detalhe de bloquear o tráfego enviado a determinadas portas ou a endereços específicos. A *firewall* incluída no Windows Server 2012 possui as características das versões anteriores, incluindo opções de configuração como a gestão remota a partir de uma máquina cliente. (Windows Firewall, n.d.)

2.16 Alta disponibilidade

Tipicamente, a missão de um servidor de rede é criticada, sendo expectável que este esteja pronto para fornecer os seus serviços aos diversos clientes da rede sem interrupções, erros ou atrasos. Os sistemas Windows Server possuem diversos mecanismos que garantem o sucesso da infra-estrutura de rede. Entre essas tecnologias destacam-se o *Failover Clustering* (Natário, Failover Clustering (I), 2011) e o *Network Load Balancing.* (Natário, Balanceamento de Carga (I), 2011)

2.17 *Backup* do Windows

O *Windows Backup* é uma ferramenta que permite executar cópias de segurança de ficheiros, volumes ou computadores inteiros e restaurar dados perdidos, quando necessário. (Windows Server Backup Step-by-Step Guide for Windows Server 2008, 2013)

Capítulo 3 – Metodologia

3.1 Pesquisa e desenvolvimento

O desenvolvimento teórico e prático deste projecto teve como base uma pesquisa realizada em livros e manuais científicos da área de Segurança Informática, assim como, artigos técnicos da Microsoft sobre a implementação e arquitectura desta tecnologia em ambiente de laboratório e práticas aconselhadas.

A componente prática deste projecto foi desenvolvida numa máquina física com as seguintes características:

ASUS N61JQ

Processador: Intel Core i7 Q720 (1.6GHz)

Memória RAM: 8GB DDR3 1600Mhz

Disco: SSD 250GB

3.2 Dificuldade encontrada

O conceito da tecnologia apresentada neste projecto assenta num ambiente de laboratório, como referido anteriormente, que pressupõe a existência de pelo menos três máquinas físicas, dois servidores e um cliente.

Tendo em conta que o projecto contempla a utilização de tecnologia Microsoft, efectuei uma pesquisa inicial nesse sentido, com vista à eventual possibilidade de utilizar três máquinas virtuais, dentro de uma máquina física. Esta metodologia assemelha-se à adoptada nas aulas de Administração de Redes.

3.3 Solução para o problema

A resposta a este problema de implementação do ambiente de laboratório foi encontrada com base na utilização de um hipervisor do tipo 2 (instalado sobre o sistema

operativo da máquina física) da empresa ORACLE, designado por Oracle VM VirtualBox Manager.

Atendendo a que um hipervisor do tipo 2 comunica com o *hardware* através do sistema operativo, foi possível efectuar as devidas implementações dos servidores e do cliente e, após vários testes e experiências, tornou-se evidente que, para efeitos de demonstração, este seria uma alternativa aceitável.

Capítulo 4 – Planeamento

Tendo sido ultrapassada a questão dos *hosts* virtuais, deu-se início ao planeamento da infra-estrutura de virtualização para o projecto e levantamento de requisitos.

A Microsoft dispõe de vários procedimentos e considerações para a implementação desta funcionalidade, e para fazer o levantamento dos requisitos a Microsoft disponibiliza informação importante que explica as vantagens e desvantagens dos mesmos para implementações com recurso a IPsec, 802.1X, VPN, DHCP e NAP-NAC. (Microsoft, 2008)

4.1 Objectivos

Para começar com o processo de implementação do NAP foi necessário identificar o objectivo de forma a poder compreender o benefício desta funcionalidade.

As implementações desenhadas para o funcionamento correcto desta funcionalidade vão ao encontro dos requisitos propostos, sendo eles: garantir a actualização dos computadores, proteger a conectividade de computadores portáteis, proteger uma rede estruturada de computadores que não estejam em conformidade, proteger uma filial de computadores que não estejam em conformidade, gestão de riscos inerentes à rede, rastreamento de conformidades de acordo com as políticas de segurança, proteger o acesso remoto e proteger os bens corporativos de computadores sem manutenção. (Microsoft, 2008)

Cabe ao administrador de redes implementar a infra-estrutura que se adequa melhor às necessidades da sua rede.

Tabela 1 - Relação de objectivos em conformidade com a implementação (Microsoft, 2008)

Objectivo da implementação NAP	Implementação IPsec	Implementação 802.1X	Implementação VPN	Implementação DHCP
Garantir computadores actualizados	Excelente	Muito Bom	Bom	Bom
Proteger conectividade dos computadores portáteis	Excelente	Bom	Bom	Bom
Proteger uma rede estruturada de computadores que não estejam em conformidade	Excelente	Excelente	Bom	Pobre
Proteger uma filial de computadores que não estejam em conformidade	Excelente	Excelente	Bom	Pobre
Gestão de riscos inerentes à rede	Excelente	Muito Bom	Bom	Bom
Rastreamento de conformidades de acordo com as políticas de segurança	Excelente	Excelente	Bom	Bom
Protecção de acesso remoto	Excelente	N/D	Excelente	N/D
Proteger os bens corporativos de computadores sem manutenção	Excelente	Muito Bom	Excelente	Pobre

4.2 Implementação

A implementação aplicada neste projecto foi com recurso ao DHCP. O motivo desta escolha, além dos objectivos anteriormente referidos, foi o facto de a mesma ser simples de implementar para efeitos de demonstração, pois não requer uma configuração

adicional a nível de *hardware* na rede e a própria estrutura de rede ser de pequena dimensão. Caso existam servidores DHCP na rede, podem ser facilmente actualizados de forma a puderem suportar a tecnologia NAP. (Microsoft, 2008)

A implementação do NAP com recurso ao DHCP obriga à instalação de certos componentes na rede:

- Um "*NAP health policy server*", executando em Windows Server 2008 R2 ou Windows Server 2008 com o "*NPS role service*" instalado;
- Um "*NAP DHCP enforcement server*", executando em Windows Server 2008 R2 ou Windows Server 2008 com o serviço DHCP e o "*NPS role service*" instalado;
- Um "*DHCP NAP-enable client computer*", executando em Windows 7, Windows Vista com Service Pack 1 (SP1), Windows XP com SP3, Windows Server 2008 ou Windows Server 2008 R2.

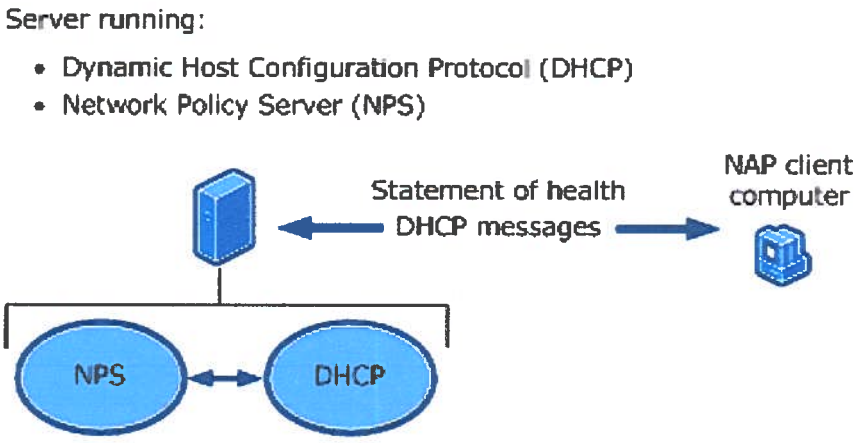

Figura 6 - Esquema de implementação genérica de NAP com recurso a DHCP (Microsoft, 2008)

4.3 Cenário

Na demonstração deste projecto, a implementação do NAP para "*DHCP network access control*" foi realizada em: um servidor com o Windows Server 2008 R2, com os serviços de DHCP e NPS instalados, um cliente com o Windows 7, com o "*NAP Agent Service*" instalado e a componente de "*DHCP Enforcement Client*" habilitada, e em um outro servidor Windows Server 2008 R2, com o propósito de ser o controlador de domínio ("DC") e DNS.

São necessários certos processos para o funcionamento correcto do NAP, como é o caso da validação de políticas, a imposição do NAP e restrições de rede, remediação e a constante monitorização para garantir a conformidade. (Microsoft, 2008)

4.3.1 Validação de políticas

Validadores de integridade do sistema ("*system health validators* – SHV") são usados pelo NPS para analisar o estatuto de integridade de um cliente. Os SHVs são incorporados nas políticas de rede que determinam acções a tomar com base no estatuto da integridade do cliente, como garantir o acesso completo à rede ou apenas restringir o acesso. Estatuto de integridade é monitorizado por "*client-side NAP components*", denominados de agentes de integridade do sistema ("*system health agents* – SHA").

NAP usa SHAs e SHVs para monitorizar, impor e remediar as configurações do cliente.

Windows Security Health Agent (WSHA) e *Windows Security Health Validator* (WSHV) foram incluídos nos sistemas operativos de forma a impor as seguintes configurações para os clientes NAP:

- O cliente tem um programa de *firewall* instalado e habilitado;
- O cliente tem um programa antivírus instalado e habilitado;
- O cliente tem o programa de antivírus actualizado;
- O cliente tem um programa de *antispyware* instalado e habilitado;
- O cliente tem o programa de *antispyware* actualizado;
- O cliente tem o "*Microsoft Update Services*" habilitado.

Neste projecto foi usado o WSHA e WSHV para requerer que o cliente tenha a *Windows Firewall* habilitada e que tenha um programa de antivírus instalado.

4.3.2 Imposição do NAP e restrições de rede

NAP possuí definições de imposição que permitem limitar o acesso à rede a clientes em inconformidade. Colocando-os numa rede restrita, adiando a restrição

para uma data posterior ou observar e registar o estatuto de integridade dos clientes compatíveis com NAP. Deste modo, as seguintes definições estão disponíveis:

- **Permitir o acesso completo**: esta opção está atribuída por defeito. Os clientes que se adequam às políticas definidas são considerados compatíveis com os requisitos de integridade da rede, e são autorizados com acesso ilimitado à rede se o pedido for autenticado e autorizado. O estatuto de conformidade/integridade do cliente NAP é registado;
- **Permitir o acesso limitado**: os clientes que estão de acordo com as políticas definidas são considerados como estando em inconformidade com os requisitos de integridade da rede e são colocados numa rede restrita;
- **Permitir o acesso completo por um tempo limitado**: os clientes que se adequam às políticas definidas estão temporariamente autorizados ao acesso completo à rede. A imposição NAP é adiada até uma data e hora específica.

Neste projecto foram criadas duas políticas de rede: uma em conformidade, que garante acesso completo a um segmento de rede na intranet, e outra em inconformidade, que demonstra a restrição à rede com recurso à configuração TCP/IP do cliente, colocando-o numa rede restrita.

4.3.3 Remediação

Os clientes que estão em inconformidade são colocados numa rede restrita e são sujeitos a um processo de remediação. Este processo actualiza o cliente para que reúna as condições de integridade. Se recursos adicionais são necessários para que os clientes em inconformidade actualizem o seu estatuto, esses recursos devem ser fornecidos na rede restrita. Por exemplo, uma rede restrita pode conter um servidor FTP que fornece actualizações dos programas antivírus para que os clientes que estão em inconformidade possam actualizar esses mesmos programas.

É possível utilizar as definições do NAP nas políticas do NPS para configurar a remediação automática, de modo a que os componentes do cliente NAP sejam actualizados automaticamente quando este esteja em inconformidade.

Neste projecto, foi demonstrado uma remediação automática. A definição "*Enable auto-remediation of client computers*" foi habilitada numa política de rede que está em inconformidade, o que causou a ligação da *Windows Firewall* sem intervenção do utilizador.

4.3.4 Constante monitorização para garantir a conformidade

NAP pode impor a compatibilidade de integridade em clientes compatíveis, que já se encontram conectados à rede. Esta funcionalidade garante que a rede está protegida em uma base contínua com as políticas de integridade e a mudança da integridade dos clientes. Os clientes são monitorizados quando há mudanças no seu estado de integridade e quando iniciam pedidos de recursos à rede.

Neste projecto, foi demonstrado uma monitorização quando o endereço emitido pelo DHCP do cliente é renovado. O cliente NAP envia um estado de integridade (SoH) com o endereço DHCP requisitado e, assim, é garantido o acesso completo ou restrito baseado no estado actual de integridade.

4.4 Networking

Para além de referir os sistemas operativos presentes nesta demonstração, é importante referir a segmentação de rede atribuída neste projecto. Esta segmentação depende de uma rede privada intranet, composta por um controlador de domínio, um membro de servidor e um cliente, e da identificação de rede privada 192.168.0.0/24.

O controlador de domínio é denominado de "DC1", e é o controlador de domínio primário para o domínio denominado de "Contoso.com". O membro de servidor é denominado de "NPS1", e é configurado com um servidor DHCP e um NPS. O cliente é denominado de "CLIENT1", e é configurado automaticamente e endereçado através de DHCP. A figura seguinte demonstra a configuração da rede presente neste projecto:

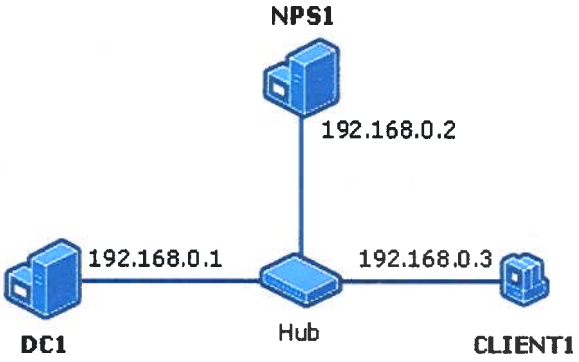

Figura 7 - Configuração de rede (Microsoft, 2008)

4.5 Alocação de recursos

Atendendo à utilização de máquinas virtuais de forma a poder efectuar a demonstração, foi necessário atribuir a cada uma recursos disponíveis da máquina física. A distribuição dos recursos foi de forma equilibrada para garantir a estabilidade das mesmas, assim como da máquina física. A seguinte tabela demonstra a alocação aplicada nesta demonstração:

Tabela 2 - Alocação de recursos

VM	OS	RAM (MB)	vHD (GB)	vCPU
DC1	Windows Server 2008 R2 Standard	2048	25	1
NPS1	Windows Server 2008 R2 Enterprise	2048	25	1
CLIENT1	Windows 7 Professional	2048	25	1

Capítulo 5 – Oracle VM VirtualBox

Como referido no capítulo 3.2, surgiu um problema com a componente prática no desenvolvimento deste projecto, como não foi possível recorrer a máquinas físicas, foi necessário virtualizar essas máquinas. A solução passou pela utilização de um hipervisor do tipo 2 denominado de Oracle VM VirtualBox Manager.

Este capítulo explica os passos necessários que foram efectuados para a criação das máquinas virtuais.

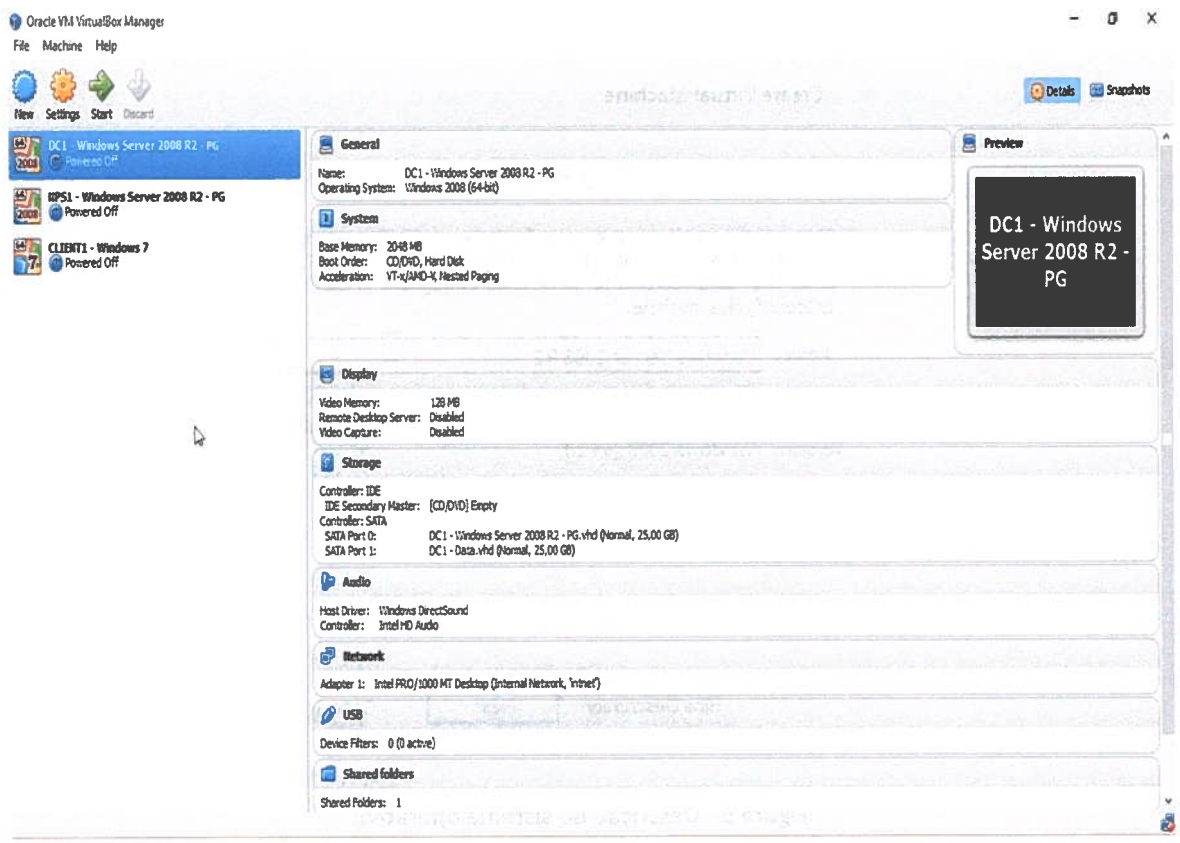

Figura 8 - Ecrã inicial do *software* Oracle VM VirtualBox Manager

5.1 Criação de uma máquina virtual

A criação de uma máquina virtual neste hipervisor é intuitiva. Para iniciar o processo foi necessário seleccionar a opção "*New*" que, por sua vez, abriu um pequeno guia de criação da máquina virtual. Este guia tem o objectivo de configurar as definições essenciais para o funcionamento correcto da máquina virtual, como é o caso das definições de *hardware*.

Uma vez seleccionada a opção "*New*", foi necessário atribuir a informação do sistema operativo que funcionará nesta máquina virtual.

Neste caso, configurou-se a máquina virtual como sendo um dos servidores usados neste projecto. Deste modo, foi atribuído o nome, o tipo e a versão do sistema operativo.

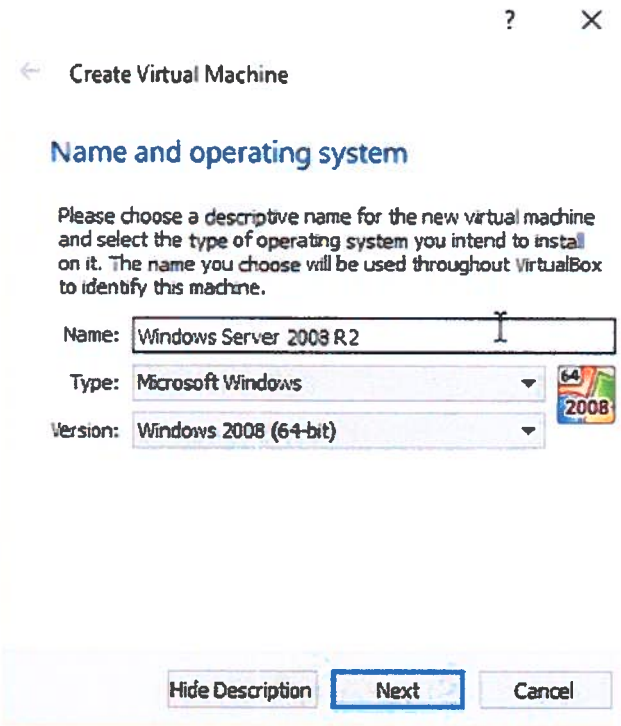

Figura 9 - Descrição do sistema operativo

Posteriormente, seleccionou-se a opção "*Next*" para o passo seguinte.

De seguida, definiu-se a quantidade de memória RAM disponível a atribuir à máquina virtual a ser criada.

Como os sistemas operativos usados neste projecto são de 64 bits disponibilizou-se a quantidade de memória RAM de 2048 Mb tendo em conta que a máquina física possuí 8Gb. A memória atribuída é recomendada para o uso neste sistema, pois vão ser necessárias três máquinas virtuais a funcionar em simultâneo com as mesmas configurações de *hardware*.

Na figura seguinte verifica-se que a quantidade de memória possível a atribuir à máquina virtual é compreendida pelo espaço a verde e o espaço a vermelho corresponde à quantidade de memória utilizada pela máquina física para o seu funcionamento. Mas como referido anteriormente, é apenas atribuído a quantidade de memória necessária para o pleno funcionamento das três máquinas virtuais.

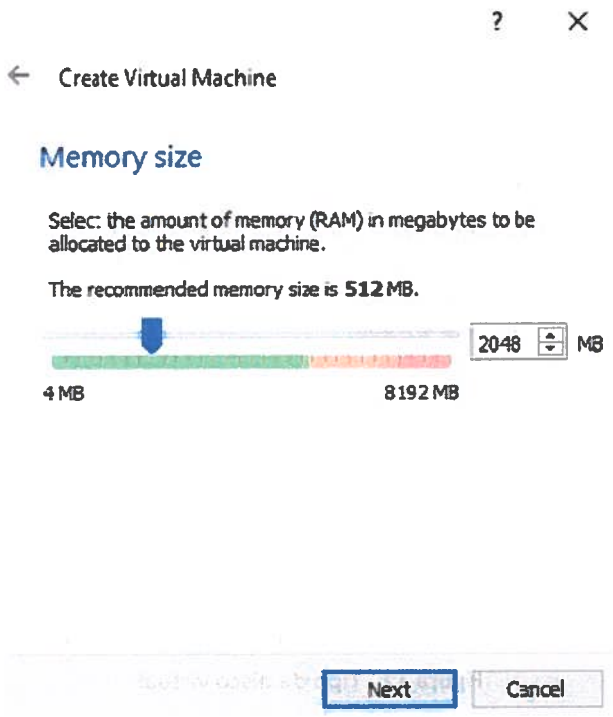

Figura 10 - Atribuição de memória RAM

Após definida a quantidade de memória a atribuir, seleccionou-se a opção "*Next*" para o passo seguinte.

Seguidamente, foi criado o disco virtual. Neste disco irá ser possível instalar e configurar o sistema operativo, assim como, as actualizações do mesmo.

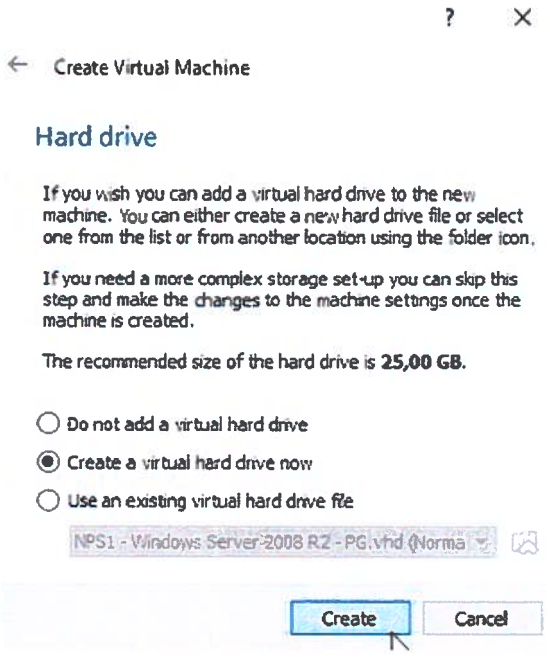

Figura 11 - Criação de disco virtual

Figura 12 - Tipo de disco virtual

Neste projecto, a unidade virtual criada foi do tipo VHD ("*Virtual Hard Disk*"), de acordo com o método adoptado nas aulas de Administração de Redes. Visto ser um disco SSD de 250Gb, limitou-se a capacidade de armazenamento para 25Gb e optou-se por seleccionar o método dinâmico de armazenamento, ou seja, apesar de determinar um limite máximo de armazenamento o disco virtual criado apenas ocupará no disco da máquina física o espaço que vai sendo ocupado por instalações de componentes dos sistemas operativos e actualizações até ao seu limite máximo atribuído.

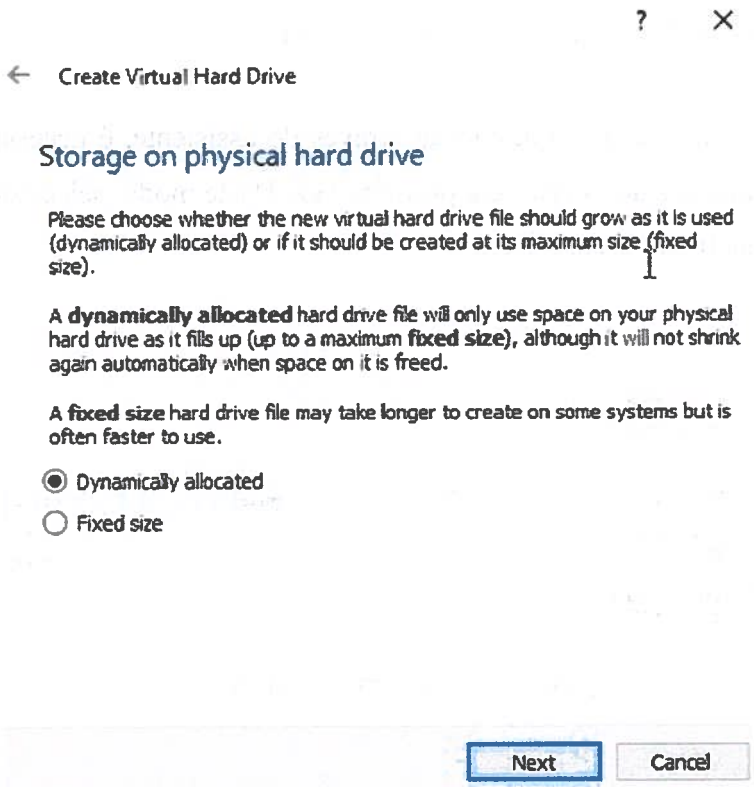

Figura 13 - Tipo de armazenamento de disco virtual

Uma vez definidas as configurações de disco virtual, seleccionou-se a opção "*Next*" e concluiu-se assim o assistente de criação da máquina virtual.

De seguida, configuraram-se as definições que não foram apresentadas no assistente de criação da máquina virtual e depois iniciou-se a máquina para proceder à instalação do sistema operativo.

5.2 Definições de uma máquina virtual

Após a criação da máquina virtual através do assistente, é necessário configurar certas definições antes de iniciar pela primeira vez. Deste modo, seleccionou-se a opção "*Settings*" na máquina virtual criada.

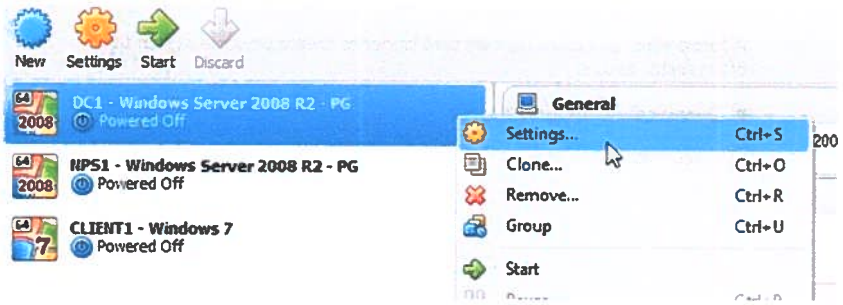

Figura 14 - Opções da máquina virtual

Uma das definições a serem configuradas dizem respeito ao "*boot order*", que vai ser necessária para começar com a instalação do sistema operativo, a opção a declarar é CD/DVD em primeiro lugar pois assim que iniciar a máquina virtual vai ser necessário introduzir o DVD de instalação do sistema operativo para prosseguir com a instalação.

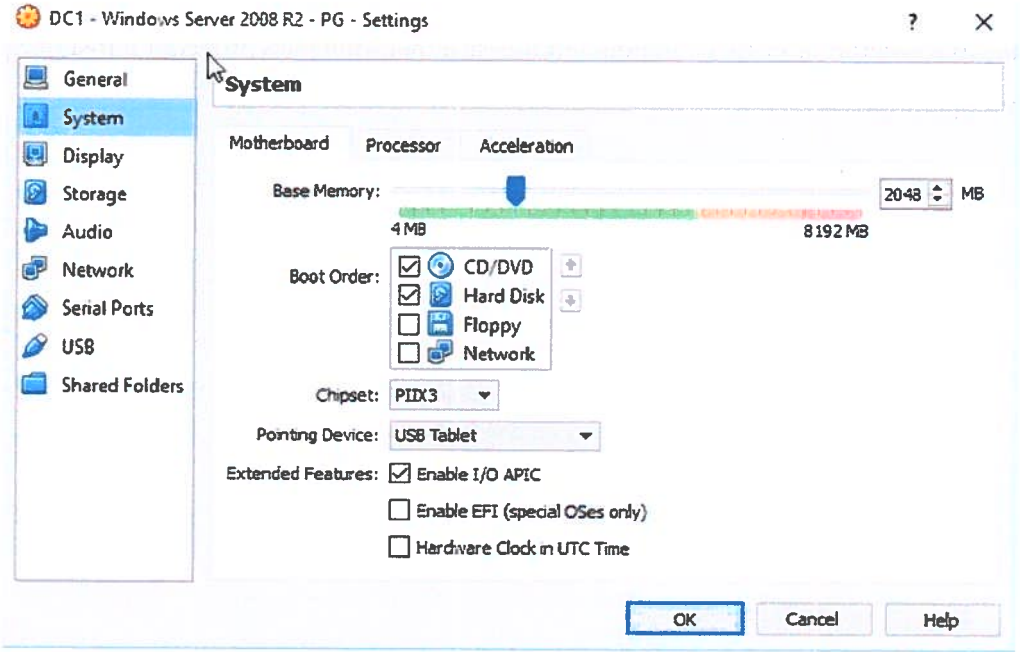

Figura 15 - Definições de sistema de máquina virtual

Outra definição a considerar é a configuração da placa de rede. Como se trata de um ambiente de laboratório onde é necessário o funcionamento em rede das três máquinas virtuais é necessário optar por uma rede interna.

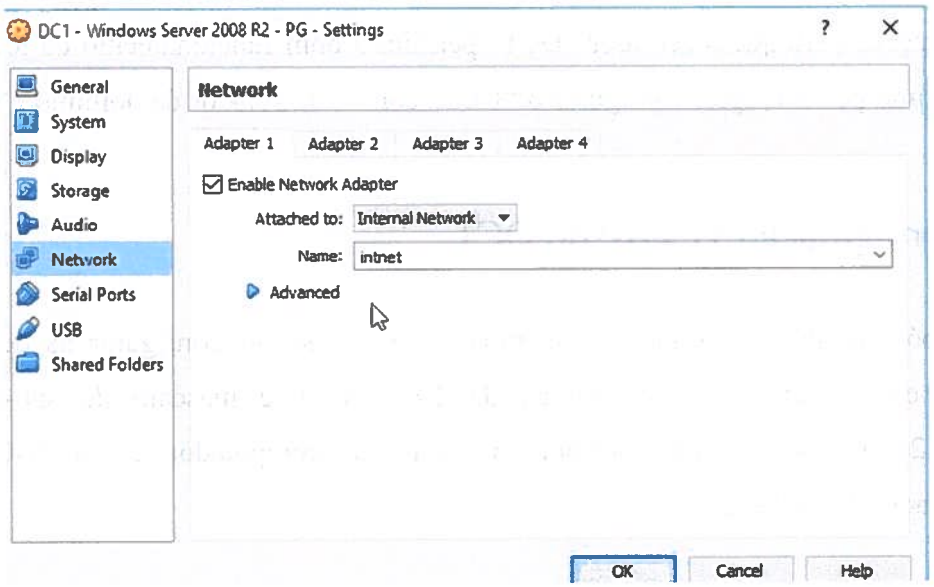

Figura 16 - Definições de rede de máquina virtual

Definidas as configurações anteriores, procedeu-se ao início da máquina virtual. Seleccionou-se a opção "*Start*" onde foi necessário introduzir o DVD de instalação do sistema operativo para prosseguir com a instalação.

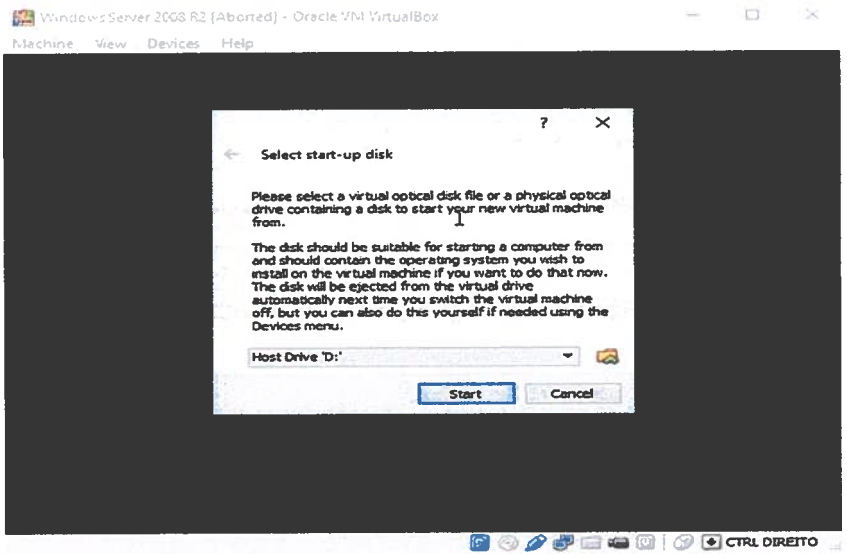

Figura 17 - "start-up disk"

Capítulo 6 – Configuração do DC1

Este capítulo tem como objectivo demonstrar a configuração do servidor de nome "DC1". Após instalação do sistema operativo, é fundamental efectuar certas configurações para que o servidor "DC1" permita o bom funcionamento da tecnologia NAP. Como por exemplo, configurar o "DC1" como controlador de domínio e servidor DNS.

6.1 Configuração TCP/IP do DC1

Após instalação do sistema operativo, foi necessário configurar as definições TCP/IP com o endereço IP estático de 192.168.0.1 e máscara de sub-rede de 255.255.255.0, assim como, atribuir o nome do computador como "DC1" nas propriedades do sistema.

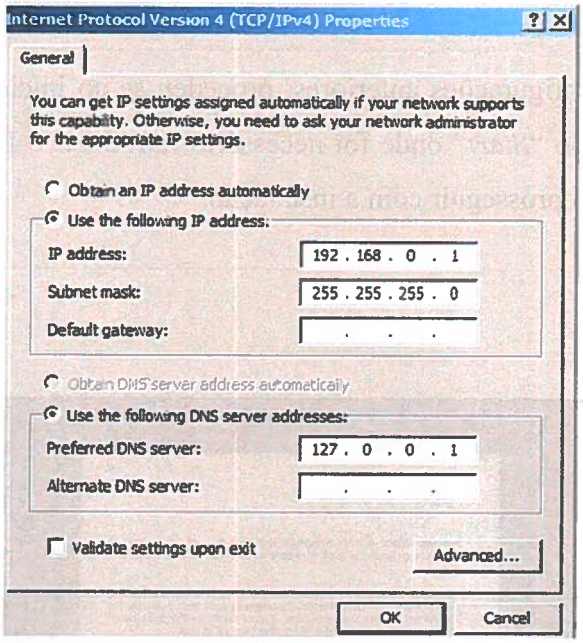

Figura 18 - Configuração TCP/IP do DC1

6.2 Configuração DC1 como controlador de domínio e servidor DNS

O servidor "DC1" apenas servirá como controlador de domínio e servidor DNS para o domínio "Contoso.com".

Para configurar "DC1" como controlador de domínio, foi necessário clicar em "*Start*" e de seguida clicar em "*Run*" e introduzir "*dcpromo*" para abrir o assistente de configuração. Neste assistente foi necessário, ainda, efectuar os seguintes passos para concluir a configuração:

- Verificar que se trata de um controlador de domínio para um novo domínio;
- Verificar que o domínio está inserido em uma nova floresta;
- Instalar o DNS;
- Introduzir "Contoso.com" em "*Full DNS name for new domain*";
- Confirmar que o "*Domain NetBIOS name*" é "CONTOSO";
- Aceitar por defeito os directórios de "*Database Folder and Log Folder*";
- Aceitar por defeito a localização para "*Shared System Volume*";
- Verificar as permissões de compatibilidade para sistemas operativos Windows Server 2008 R2;
- Atribuir e confirmar *password* de acesso;
- Confirmar através de uma forma sumariada as configurações efectuadas;
- Reiniciar o computador.

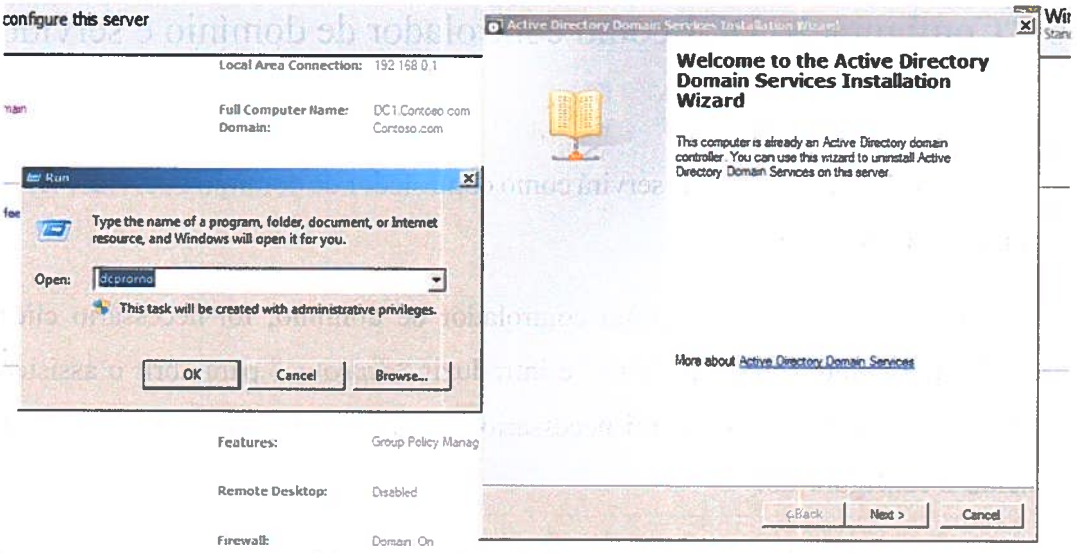

Figura 19 - Assistente do Active Directory Domain Services

Após reiniciar, a autenticação no sistema operativo foi efectuada com a conta de administrador no domínio "CONTOSO".

Figura 20 - Autenticação CONTOSO\Administrator

6.3 Criar conta de utilizador no *Active Directory*

O passo seguinte diz respeito à criação de uma conta de utilizador, onde vai ser possível fazer a autenticação da mesma no servidor NPS1 e no CLIENT1 para os devidos efeitos.

Para começar, clicou-se em "*Start*", seleccionou-se "*Administrative Tools*" e clicou-se em "*Active Directory Users and Computers*".

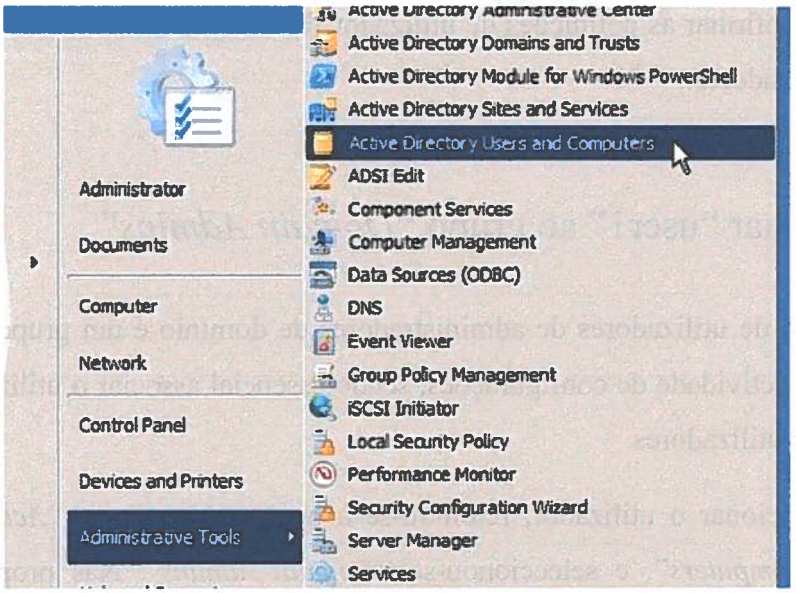

Figura 21 - Active Directory Users and Computers

De seguida, seleccionou-se "Contoso.com" com o botão direito para visualizar as opções disponíveis. A opção adoptada foi "*New*", onde se seleccionou "*User*" para prosseguir.

Nas opções seguintes, atribuiu-se o nome completo como "User1 User" e "User1" como nome de autenticação, e também definiu-se a palavra-passe do utilizador.

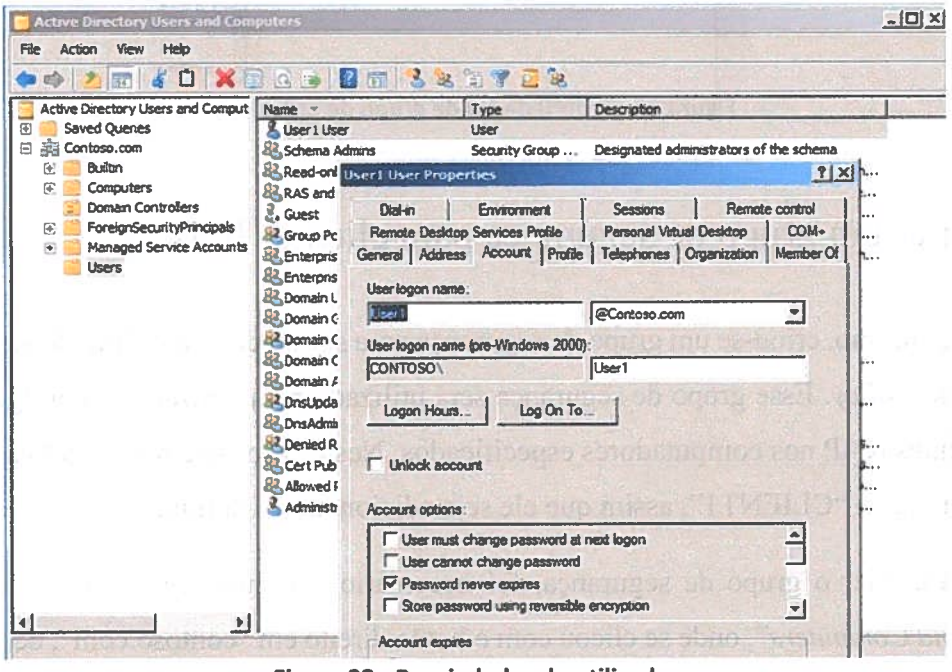

Figura 22 - Propiedades de utilizador

Após confirmar as definições de utilizador foi necessário associar o mesmo a um grupo de utilizadores.

6.4 Adicionar "user1" ao grupo "*Domain Admins*"

O grupo de utilizadores de administradores de domínio é um grupo que é usado para todas as actividade de configurações, sendo essencial associar o utilizador criado a esse grupo de utilizadores.

Para adicionar o utilizador, retomou-se à opção "*Users*", no "*Active Directory Users and Computers*", e seleccionou-se "*Domain Admins*". Nas propriedades dos "*Domain Admins*", clicou-se no separador "*Members*" e de seguida clicou-se em "*Add*". Deste modo, introduziu-se "User1" na janela dos nomes e clicou-se em "*Ok*".

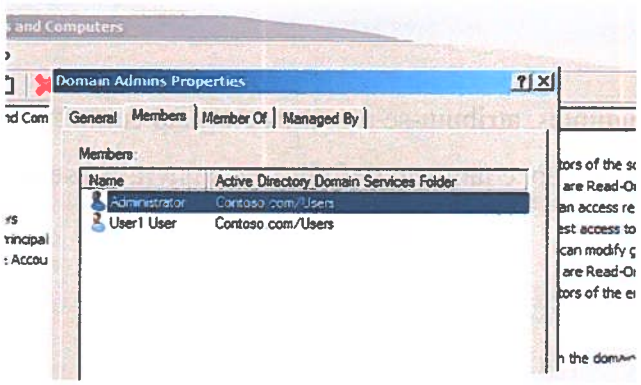

Figura 23 - Propriedades de grupo de utilizador

6.5 Criar um grupo de segurança para clientes NAP

Por último, criou-se um grupo de segurança para ser usado como filtro de segurança no *Group Policy*. Esse grupo de segurança será utilizado para verificar as configurações dos clientes NAP nos computadores especificados. Neste caso, será adicionado ao grupo de segurança o "CLIENT1", assim que ele seja adicionado ao domínio.

Para criar o grupo de segurança, foi necessário continuar em "*Active Directory Users and Computers*", onde se clicou com o botão direito em "contoso.com", de seguida em "*New*" e clicou-se em "*Group*". Na janela seguinte, introduziu-se o nome de grupo

"NAP client computers" e seleccionou-se o "*Group scope*" como "*Global*" e o "*Group type*" como "*Security*" e clicou-se em "*Ok*".

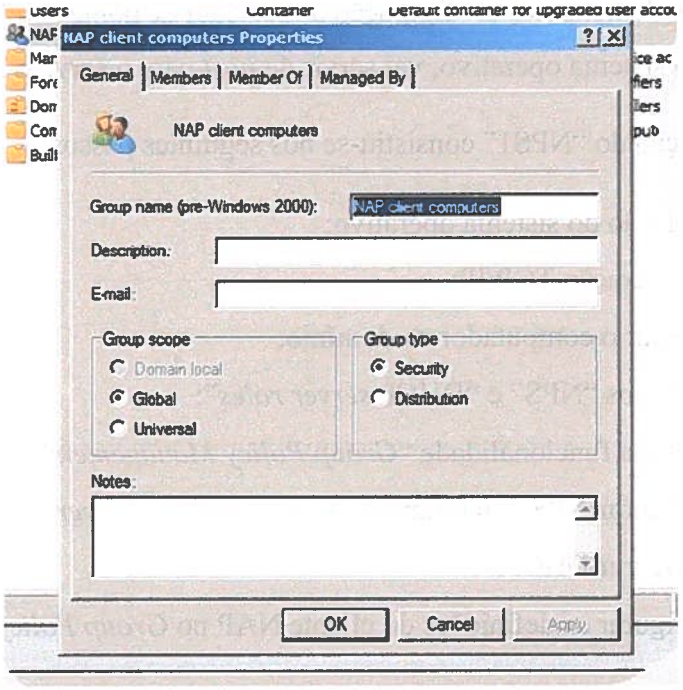

Figura 24 - Propriedades de grupo de segurança

Capítulo 7 – Configuração do NPS1

Este capítulo demonstra a configuração do servidor de nome "NPS1". Este servidor, após instalação do sistema operativo, vai servir de *host* para o serviço NPS.

A configuração do "NPS1" consistiu-se nos seguintes passos:

- Instalação do sistema operativo;
- Configuração TCP/IP;
- Associar o computador ao domínio;
- Instalar os "NPS" e "DHCP *server roles*";
- Instalar a funcionalidade "*Group Policy Management*";
- Configurar NPS como um "*NAP health policy server*";
- Configurar DHCP;
- Configurar as definições do cliente NAP no *Group Policy*.

7.1 Configuração TCP/IP do NPS1

Após instalação do sistema operativo foi necessário configurar as definições TCP/IP do sistema.

À semelhança do capítulo 6.1, o método de configuração apenas difere no uso de um endereço de IP diferente ao do "DC1". O endereço de IP a ser usado no "NPS1" foi o 192.168.0.2 e máscara de sub-rede 255.255.255.0. Também foi necessário alterar o endereço do servidor DNS para 192.168.0.1, após confirmar estes dados clicou-se em "*Ok*".

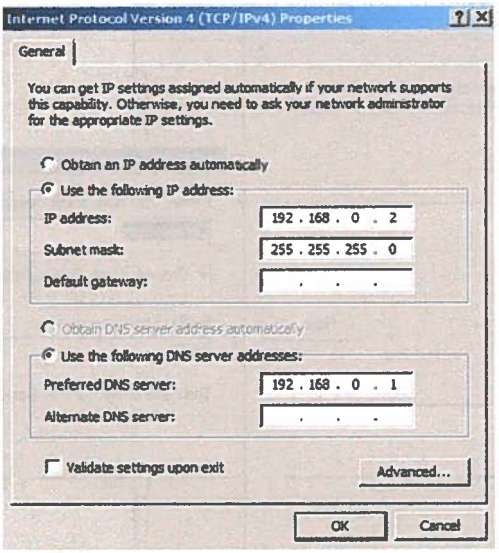

Figura 25 - Configuração do TCP/IP do NPS1

Após a configuração do TCP/IP, foi necessário verificar a comunicação entre o "NPS1" e o "DC1", para tal, fez-se *ping* no "NPS1". Para confirmar esta comunicação, clicou-se em "*Start*", de seguida em "*Run*", introduziu-se "*cmd*" e pressionou-se "ENTER". Na janela de comando que entretanto abriu, introduziu-se "*ping DC1*" e verificou-se uma resposta de "*Reply from 192.168.0.1*".

7.2 Adicionar NPS1 ao domínio "contoso.com"

Para começar, abriu-se o "*Server Manager*" e clicou-se em "*Change System Properties*". Este procedimento permitiu a abertura da janela "*System Properties*", permitindo, por sua vez, introduzir o nome de computador para "NPS1". Na janela "*Computer Name/Domain Changes*", na opção "*Member of*", seleccionou-se "*Domain*" e introduziu-se "Contoso.com". De seguida, clicou-se em "*More*" para introduzir "Contoso.com" em "*Primary DNS suffix of this computer*". Confirmadas estas alterações, clicou-se em "*Ok*". Este procedimento gerou o aparecimento de uma janela que permitiu introduzir o nome de utilizador e palavra-passe. Os dados de autenticação do utilizador introduzidos foram os do utilizador que foi adicionado ao grupo dos "*Domain Admins*", ou seja, o "User1".

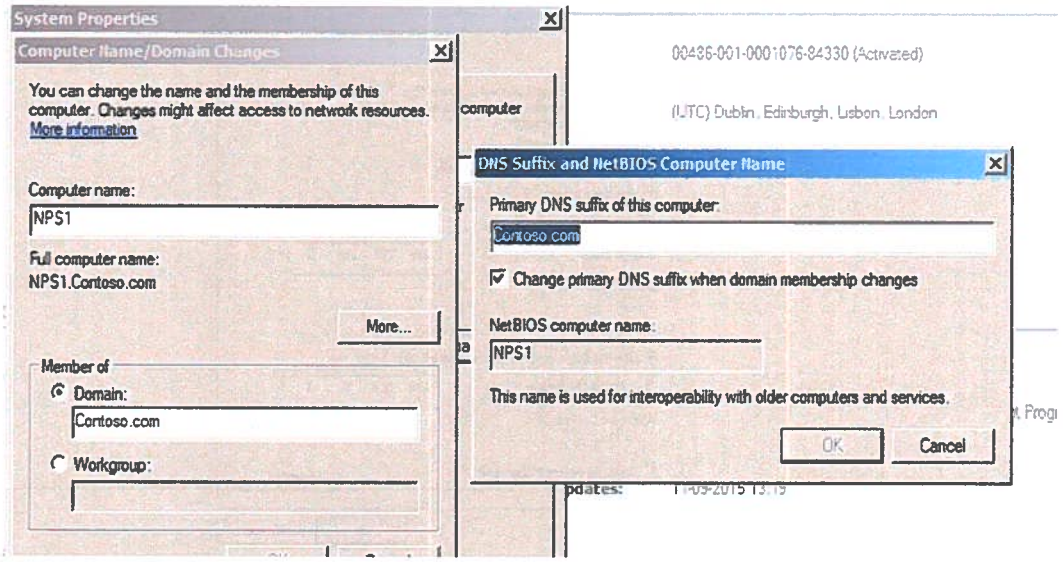

Figura 26 - Propriedades de sistema NPS1

Confirmados os dados do utilizador, foi necessário reiniciar o computador. De seguida, seleccionou-se "*Switch User*" e clicou-se em "*Other User*". Por fim, introduziu-se "CONTOSO" no campo de domínio e "User1" no nome de utilizador de conta, de modo a proceder à autenticação do utilizador.

Figura 27 - Autenticação CONTOSO\User1

7.3 Instalar NPS e DHCP *server roles*

Para proceder à instalação do NPS e DHCP *server roles* no "NPS1", clicou-se em "*Start*" e posteriormente em "*Server Manager*". Em "*Roles Summary*", clicou-se em "*Add roles*" e de seguida em "*Next*".

Na janela seguinte e na página "*Select Server Roles*", seleccionaram-se as opções "*DHCP Server*" e "*Network Policy and Access Services*" e clicou-se em "*Next*".

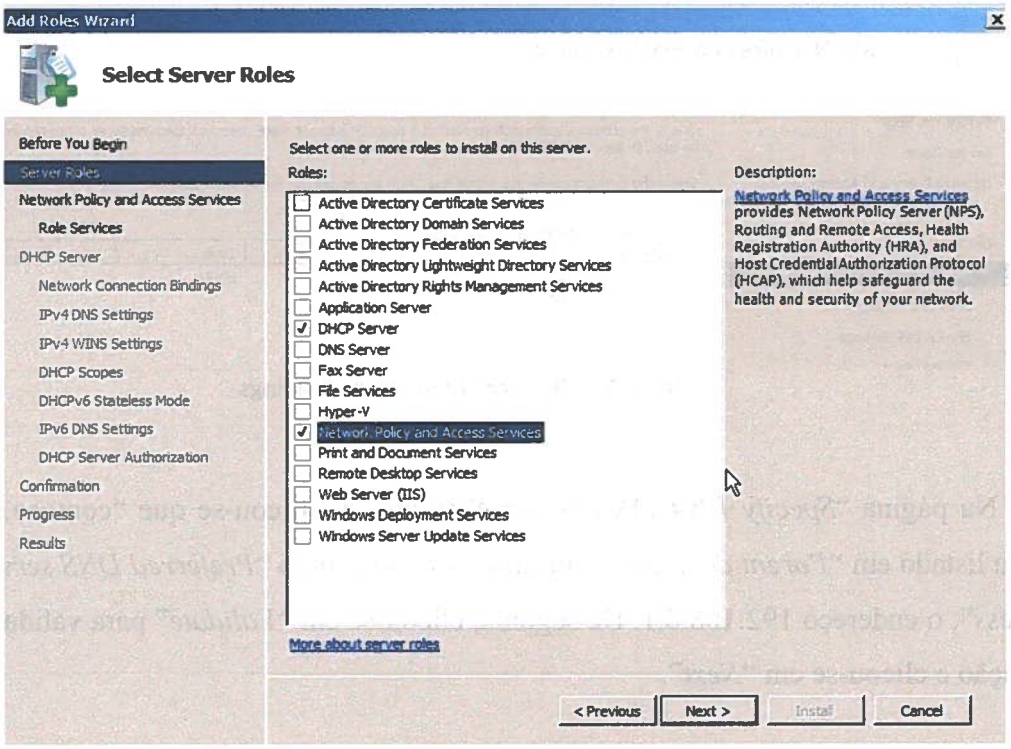

Figura 28 - Server Roles

Na página "*Select Role Services*", seleccionou-se a opção "*Network Policy Server*" e clicou-se em "*Next*".

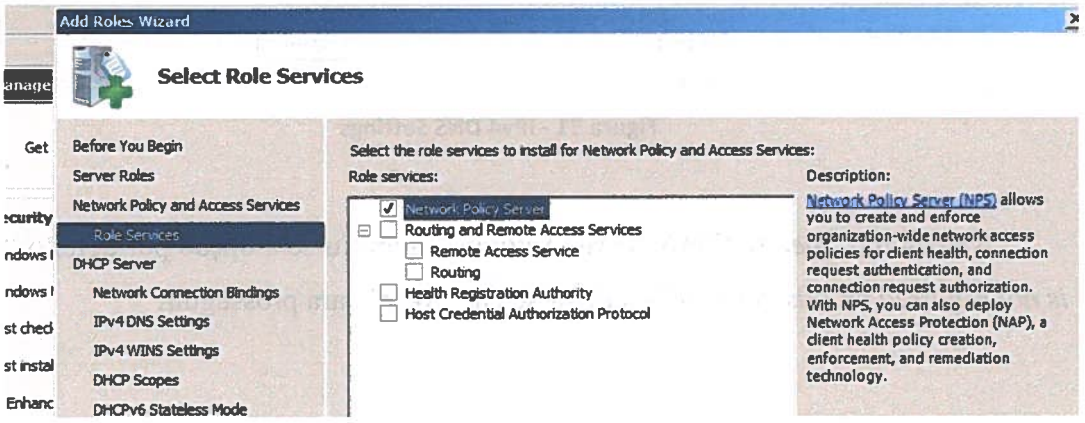

Figura 29 - Role Services

Na página "*Select Network Connection Bindings*", verificou-se que 192.168.0.2 foi seleccionado, deste modo, clicou-se em "*Next*" para continuar com o seguinte passo.

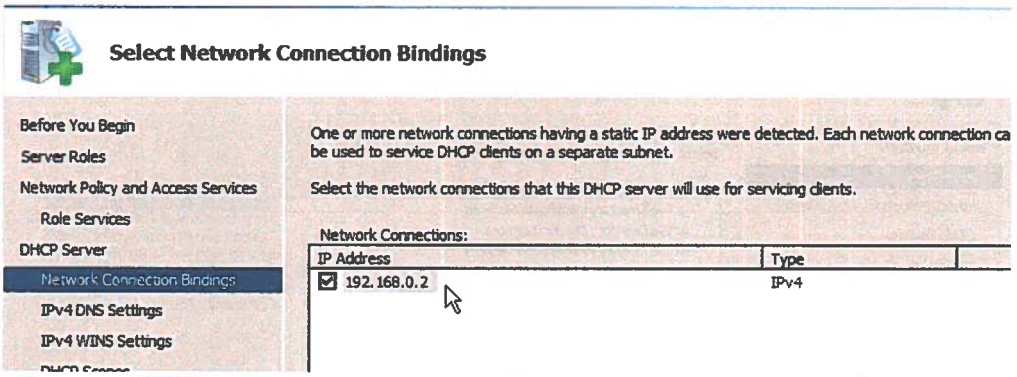

Figura 30 - Network Connection Bindings

Na página "*Specify IPv4 DNS Server Settings*", verificou-se que "contoso.com" estava listado em "*Parent domain*" e introduziu-se, no campo "*Preferred DNS server IP address*", o endereço 192.168.0.1. De seguida, clicou-se em "*Validate*" para validar esta operação e clicou-se em "*Next*".

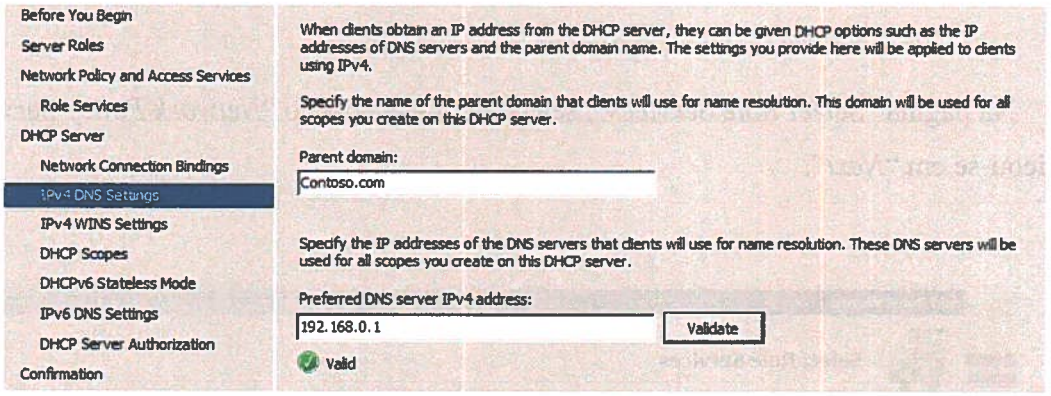

Figura 31 - IPv4 DNS Settings

Na página "*Specify WINS Server Settings*", admitiu-se a opção por defeito "*WINS is not required on this network*" e clicou-se em "*Next*" para prosseguir.

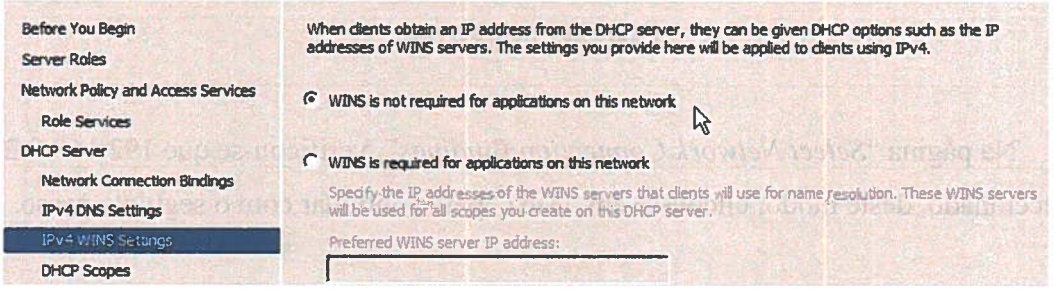

Figura 32 - IPv4 WINS Settings

Na página "*Add or Edit DHCP Scopes*", clicou-se em "*Add*" e na janela "*Add Scope*" introduziu-se NAP Scope em "*Scope Name*", 192.168.0.3 em "*Starting IP Address*", 192.168.0.10 em "*Ending IP Address*", 255.255.255.0 em "*Subnet Mask*" e por fim habilitou-se a opção "*Active this scope*". Confirmada esta informação, clicou-se em "*Ok*" e de seguida em "*Next*" para o passo seguinte.

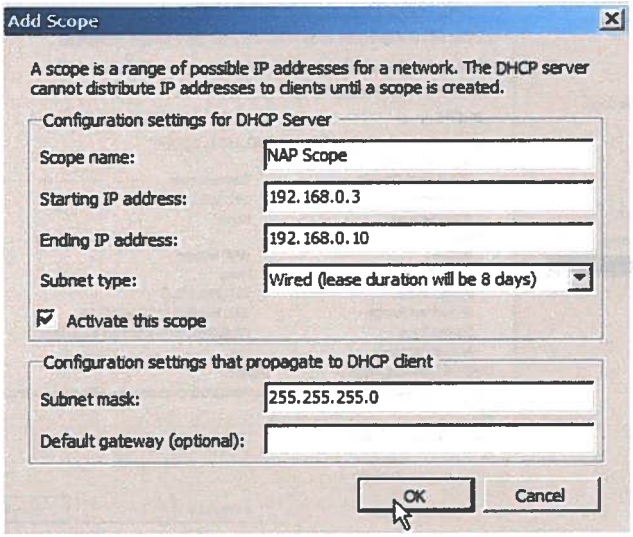

Figura 33 - Add Scope

Na página "*Configure DHCPv6 Stateless Mode*", seleccionou-se "*Disable DHCPv6 stateless mode for this server*" e clicou-se em "*Next*".

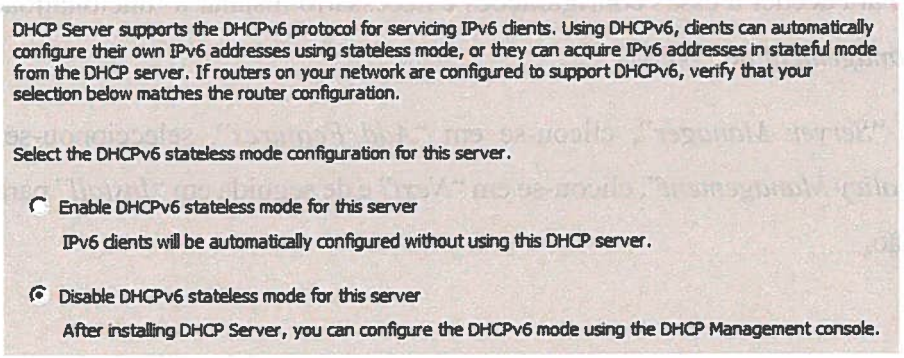

Figura 34 - DHCPv6 Stateless Mode

Na página "*Authorize DHCP Server*", seleccionou-se "*Use current credentials*", verificou-se que "CONTOSO\user1" foi exibido em "*Username*" e clicou-se em "*Next*".

De seguida, confirmaram-se as configurações efectuadas na página "*Confirmation*" e clicou-se em "*Install*" para concluir a instalação dos *server roles*.

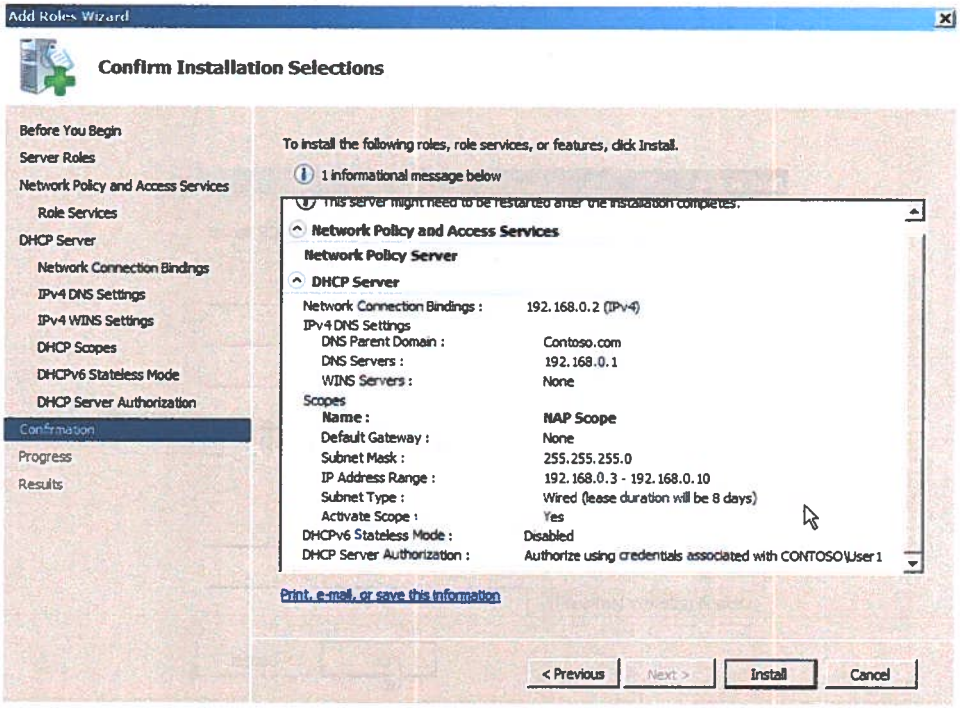

Figura 35 - Confirm Installation Selections

7.4 Instalar *Group Policy Management*

O *Group Policy* será usado para configurar as definições de clientes NAP neste projecto. Para aceder a essas configurações é necessário instalar a funcionalidade *Group Policy Management* no "NPS1".

Em "*Server Manager*", clicou-se em "*Add Features*", seleccionou-se a opção "*Group Policy Management*", clicou-se em "*Next*" e de seguida em "*Install*" para concluir a instalação.

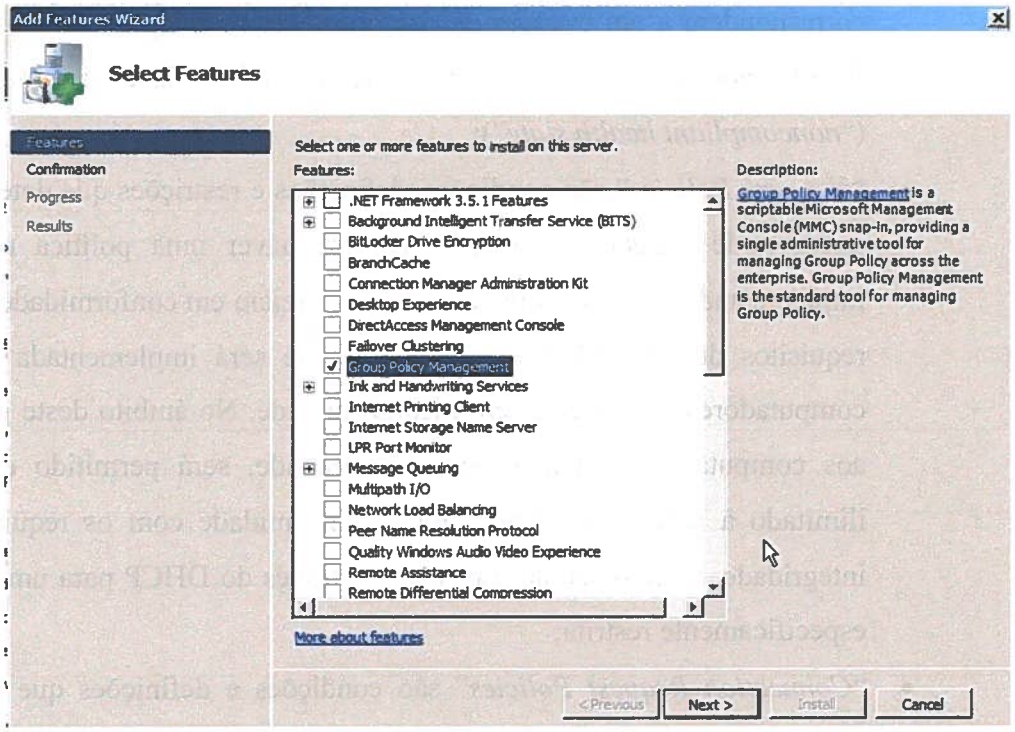

Figura 36 - Group Policy Management feature

7.5 Configurar o NPS como um "*NAP health policy server*"

Para configurar o NPS como um "*NAP health policy server*" o "NPS1" deverá validar a integridade do sistema de acordo com os requisitos de integridade da rede configurada.

Neste projecto, a configuração do NPS como um "*NAP health policy server*" foi executada através de um assistente. Este assistente permite ajudar a configurar cada componente NAP a trabalhar de acordo com o método de imposição definido. Esses componentes serão mostrados no NPS e incluí:

- "*System Health Validators*" (SHVs) definem a configuração de requisitos para computadores que tentam conectar-se à rede. No âmbito deste projecto, o WSHV apenas será configurado para requerer que a *Firewall* esteja ligada;
- "*Health Policies*" permite definir quais SHVs são avaliados e como são utilizados na validação da configuração de computadores que tentam conectar-se à rede. De acordo com os resultados das verificações SHV, as políticas de conformidade permitem classificar o estatuto de conformidade do cliente. As duas políticas de conformidade testadas neste projecto

correspondem a um estatuto de conformidade de integridade ("*compliant health state*") e a um estatuto de inconformidade de integridade ("*noncompliant health state*");

- "*Network Policies*" são condições, definições e restrições que determinam quem pode conectar-se à rede. Deverá haver uma política que será implementada para os computadores que estejam em conformidade com os requisitos de integridade e uma outra que será implementada para os computadores que estejam em inconformidade. No âmbito deste projecto, aos computadores clientes em conformidade, será permitido o acesso ilimitado à rede, aos clientes em inconformidade com os requisitos de integridade, terão o seu acesso restrito através do DHCP para uma *subnet* especificamente restrita;
- "*Connection Request Policies*" são condições e definições que validam pedidos para acesso à rede e gerem onde essa validação é executada. Neste projecto, a política de pedido de conexão a ser usada requer DHCP como servidor de acesso de rede para autenticação de cliente;
- "*RADIUS Clients and Servers*", clientes RADIUS são servidores de acesso à rede. Se se especificar um cliente RADIUS então um servidor RADIUS correspondente será necessário, no dispositivo do cliente RADIUS. Servidores "*Remote DHCP*" são configurados como clientes RADIUS no NPS. Não será necessário usar um "*Remote DHCP*" neste projecto, pois não será necessário efectuar uma configuração de clientes e servidores RADIUS;
- "*Remediation Server Groups*" é permitido ao administrador de rede especificar os servidores que ficam disponíveis para clientes NAP que estejam em inconformidade para que eles entrem num estado de remediação e, deste modo, possam voltar ao seu estado de conformidade com os requisitos de integridade. Se esses servidores são requisitados, eles automaticamente ficam disponíveis para os computadores com acesso restrito à *subnet* quando são adicionados aos grupos de servidores de remediação. Neste projecto, e para efeitos de demonstração, será usado um grupo de servidor de remediação que provém de serviços de domínio para um cliente com acesso restrito à rede.

7.5.1 Configuração NAP com um assistente

O assistente de configuração NAP permite definir o NPS como um "*NAP health policy server*". Este assistente, contém definições específicas para o método de imposição adoptado e automaticamente cria políticas NAP customizadas.

Para configurar o NPS utilizando um assistente NAP, foi necessário clicar em "*Start*", de seguida em "*Run*", onde se introduziu "*nps.msc*", e pressionou-se "ENTER". No painel lateral do "*Network Policy Server*", clicou-se em "*NPS (Local)*" e no painel de detalhes clicou-se em "*Configure NAP*" para iniciar o assistente.

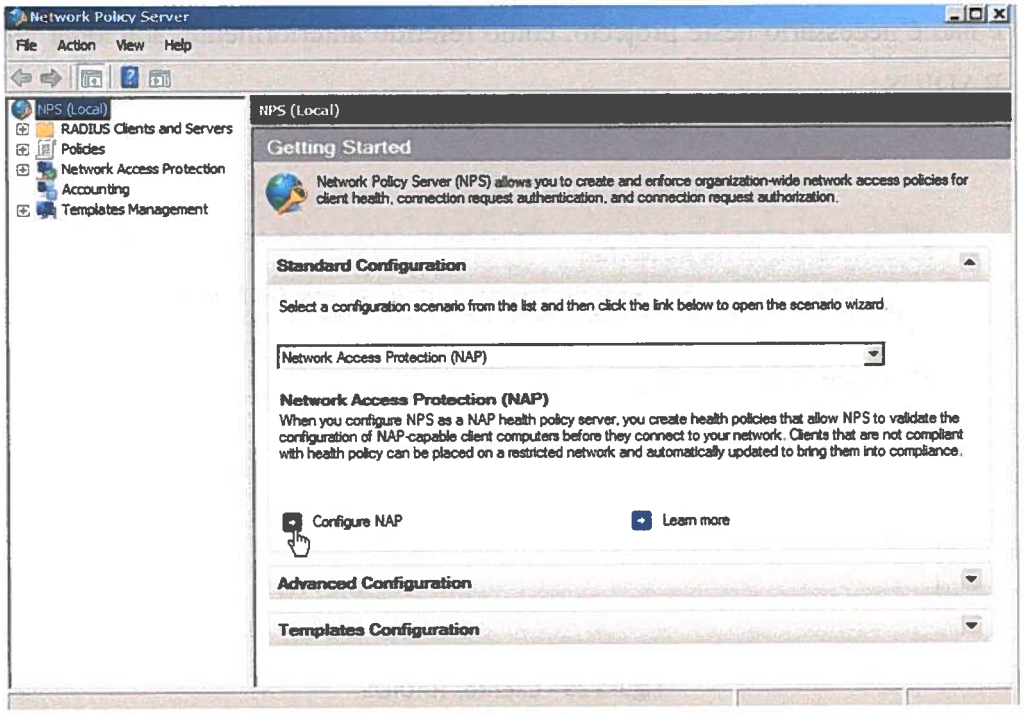

Figura 37 - NPS (Local)

Na página "*Select Network Connection Method for Use with NAP*", por baixo de "*Network connection method*" seleccionou-se "*Dynamic Host Configuration Protocol (DHCP)*" e então clicou-se em "*Next*".

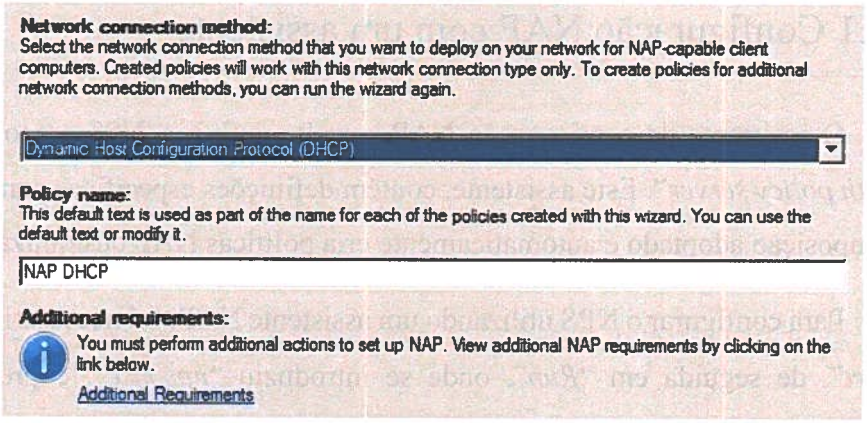

Figura 38 - Network connection method

Na página "*Specify NAP Enforcement Server Running DHCP*", clicou-se em "*Next*" porque este "*NAP health policy server*" tem o DHCP instalado localmente e não é necessário neste projecto, como referido anteriormente, adicionar clientes RADIUS.

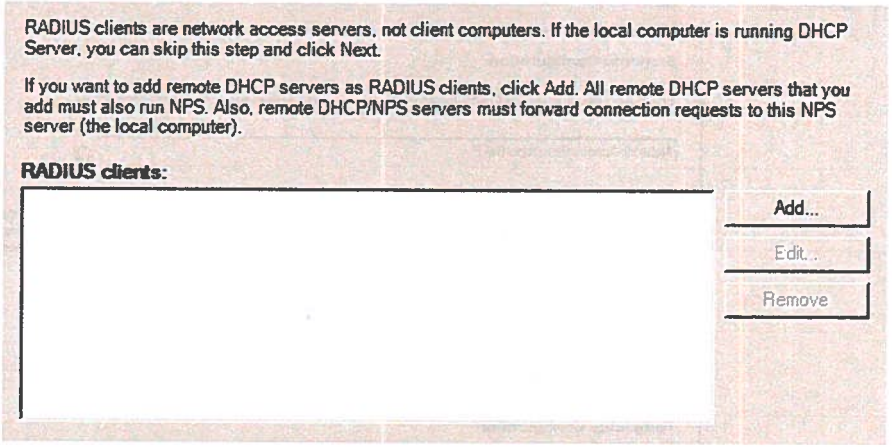

Figura 39 - Clientes RADIUS

Tendo em conta que neste projecto apenas será usado um DHCP *scope,* pelo que não será necessário *scopes* adicionais, procedeu-se da seguinte forma: na página "*Specify DHCP Scopes*", clicou-se em "*Next*".

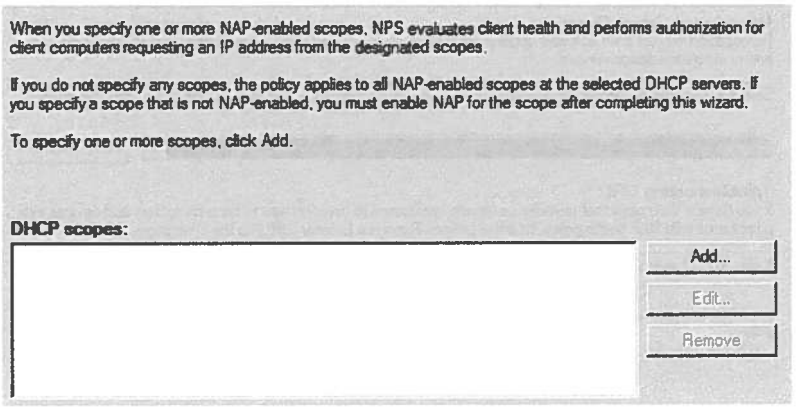

Figura 40 - DHCP Scopes

Tendo em conta que para este projecto não é necessário a configuração de grupos, procedeu-se da seguinte forma: na página "*Configure User Groups and Machine Groups*" clicou-se em "*Next*".

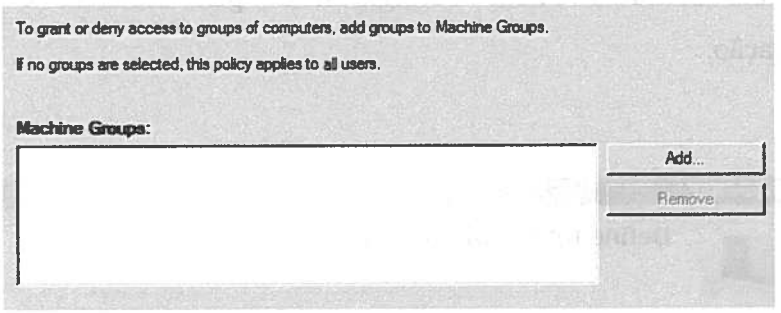

Figura 41 - Machine Groups

Tendo em conta, que os servidores de remediação serão configurados posteriormente, procedeu-se da seguinte forma: na página "*Specify a NAP Remediation Server Group*" clicou-se em "*Next*".

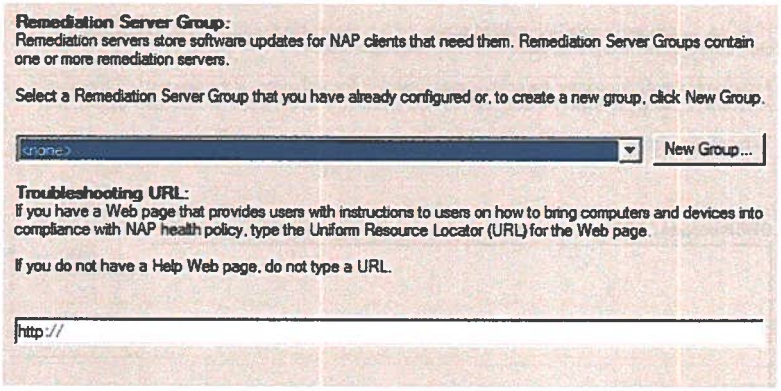

Figura 42 - Remediation Server Group

Na página "*Define NAP Health Policy*", verificou-se que as opções "*Windows Security Health Validator*" e "*Enable auto-remediation of client computers*" estão habilitadas, deste modo clicou-se em "*Next*".

Finalmente, clicou-se em "*Finish*" na página "*Completing NAP Enforcement Policy and RADIUS Client Configuration*" para finalizar o assistente de configuração.

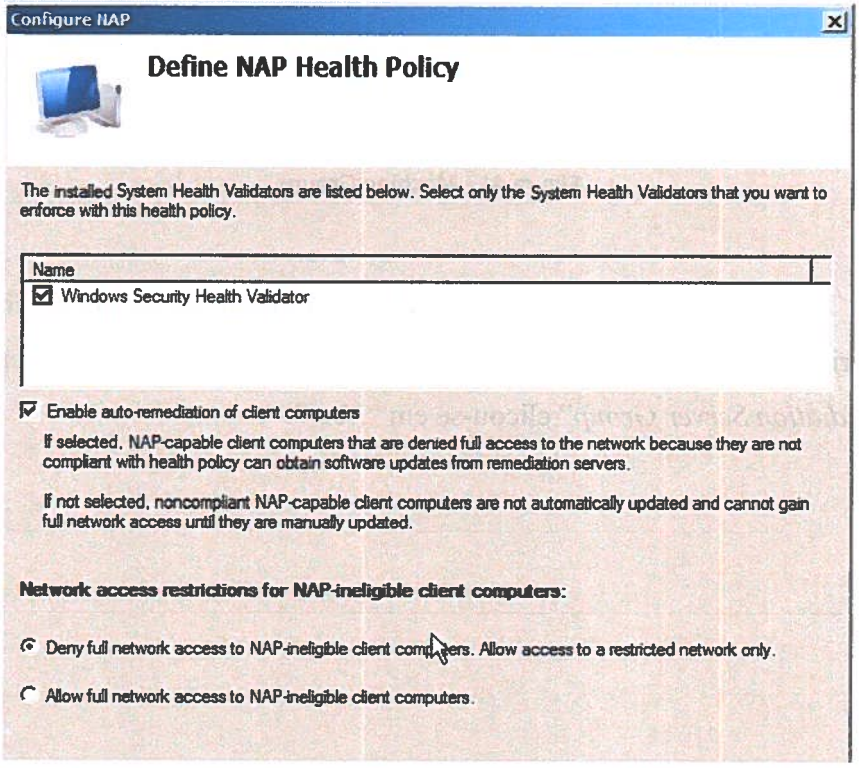

Figura 43 - NAP Health Policy

7.5.2 Configuração de SHVs

SHVs definem os requisitos de configuração para os computadores que conectam à rede. Para esta demonstração, o WSHV será configurado para requisitar somente que a *Windows Firewall* esteja ligada.

Para começar a configurar os validadores de integridade do sistema no "*Network Policy Server*", acedeu-se a "*Network Access Protection*", "*System Health Validators*", "*Windows Security Health Validator*" e por fim "*Settings*".

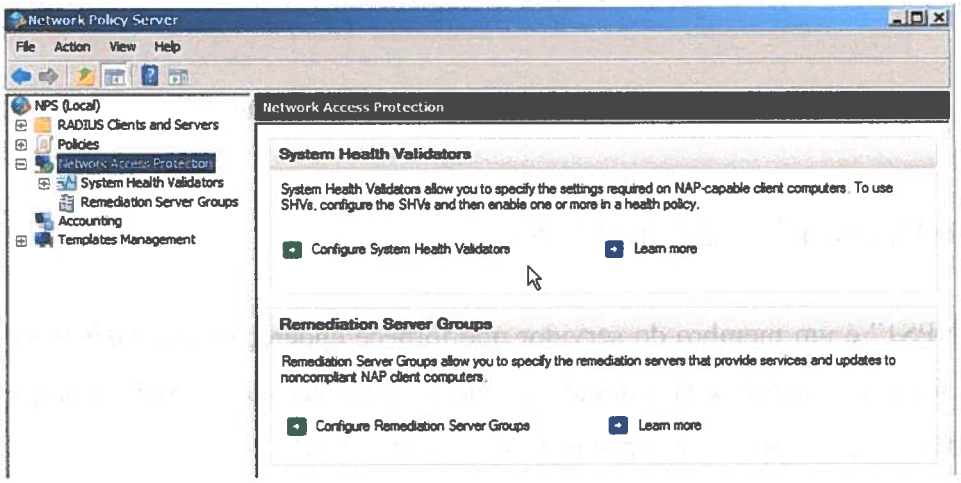

Figura 44 - Configure SHVs

No painel de detalhes, fez-se um duplo clique em "*Default Configuration*", de modo a disponibilizar a janela "*Windows Security Health Validator*", no painel lateral da janela seleccionou-se a opção "*Windows 7/Windows Vista*" e no painel "*Choose policy settings for Windows Security Health Validator*" retirou-se os vistos das caixas de selecção, com a excepto da opção "*A firewall is enable for all network conections*". Por fim, clicou-se em "*Ok*" para fechar a janela "*Windows Security Health Validator*" e fechou-se a consola do "*Network Policy Server*"

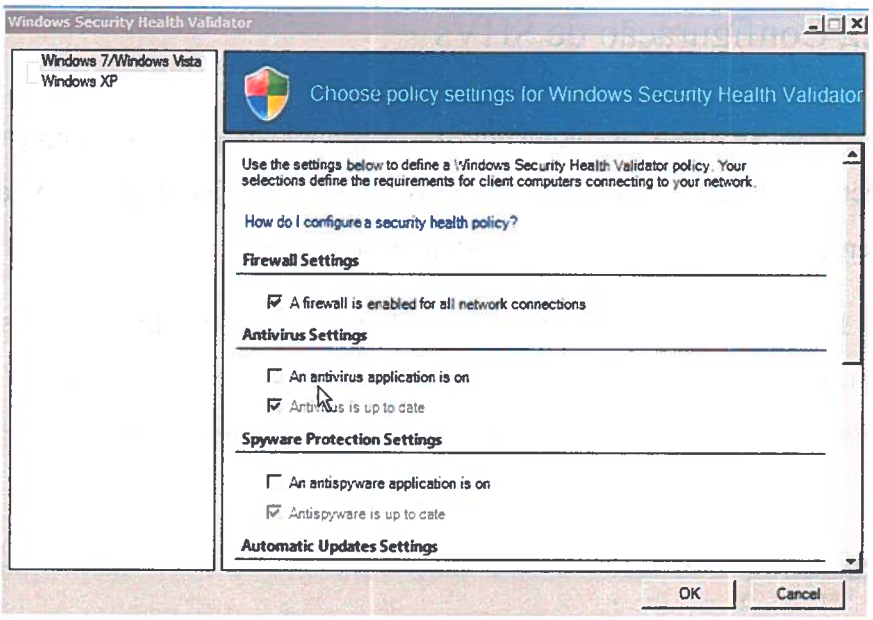

Figura 45 - Windows Security Health Validator

7.6 Configurar DHCP no NPS1

"NPS1" é um membro do servidor que fornece endereçamento DHCP. O serviço DHCP foi parcialmente configurado durante a instalação do *Server Manager*. Neste capítulo serão configuradas as opções de *scope* para o NAP.

Para começar as configurações, foi necessário abrir a consola DHCP, clicou-se em "*Start*" e em "*Run*", onde se introduziu "*dhcpmgmt.msc*" e pressionou-se em "ENTER".

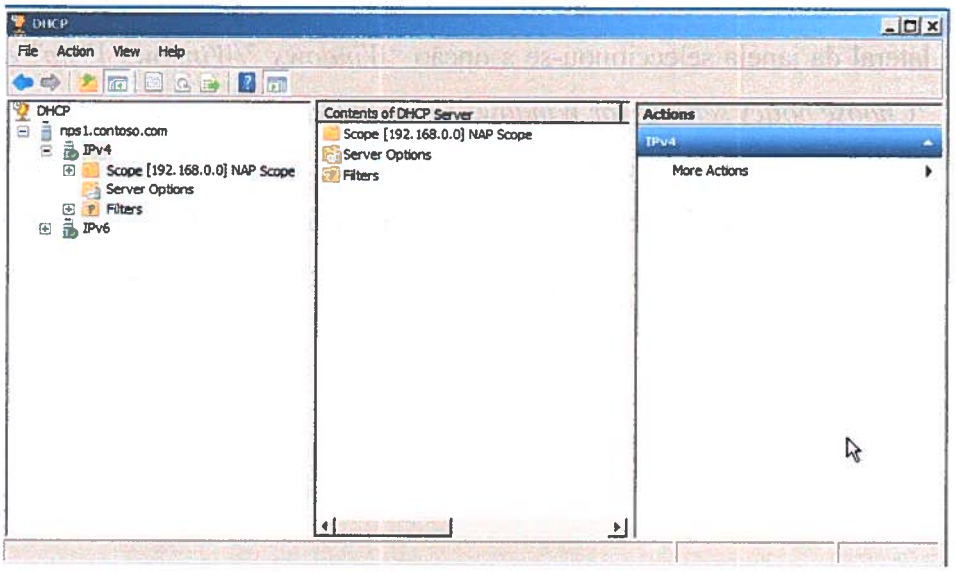

Figura 46 - Consola DHCP

7.6.1 Habilitar as definições NAP para o *scope*

É necessário habilitar o perfil por defeito do NAP para o *scope* NAP.

Na consola DHCP fez-se duplo clique em "*nps1.contoso.com*" e depois duplo clique em "*IPv4*". De seguida, clicou-se com o botão direito sobre "*Scope [192.168.0.0] NAP Scope*" e clicou-se em "*Properties*".

No separador "*Network Access Protection*" das propriedades do *scope*, em "*Network Access Protection Settings*" seleccionou-se "*Enable for this scope*" e verificou-se que a opção "*Use default Network Access Protection profile*" estava seleccionada, dessa forma clicou-se em "*Ok*".

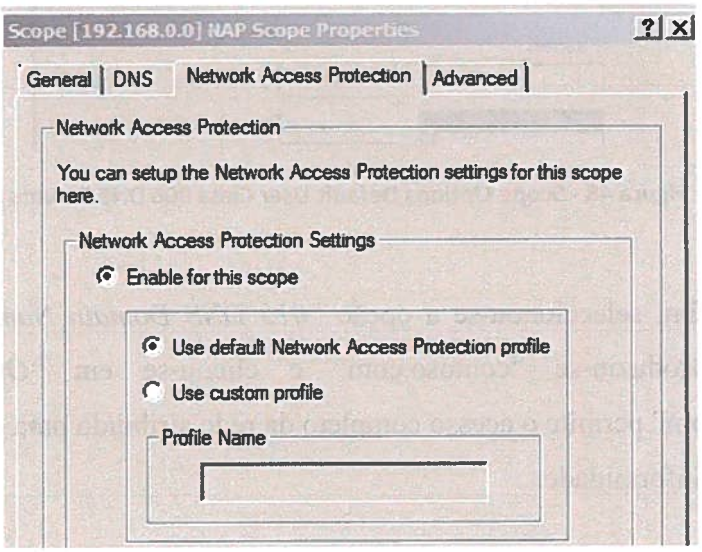

Figura 47 - NAP Scope Properties

7.6.2 Configurar a classe de defeito do utilizador

Neste ponto, configuraram-se as opções de *scope* para a classe de defeito do utilizador. Estas opções são usadas quando um cliente computador em conformidade tenta aceder à rede e obtém um endereço IP do servidor DHCP.

Para iniciar a configuração das opções do scope da classe de defeito do utilizador, na consola DHCP clicou-se com o botão direito em "*Scope Options*" no "*Scope [192.168.0.0] NAP Scope*" e clicou-se em "*Configure Options*".

No separador "*Advanced*" do "*Scope Options*", verificou-se que a opção "*Default User Class*" foi seleccionada em "*User Class*". De seguida, seleccionou-se a opção "*006 DNS Servers*" e em "*IP Address*" introduziu-se 192.168.0.1 e, desta forma, clicou-se em "*Add*".

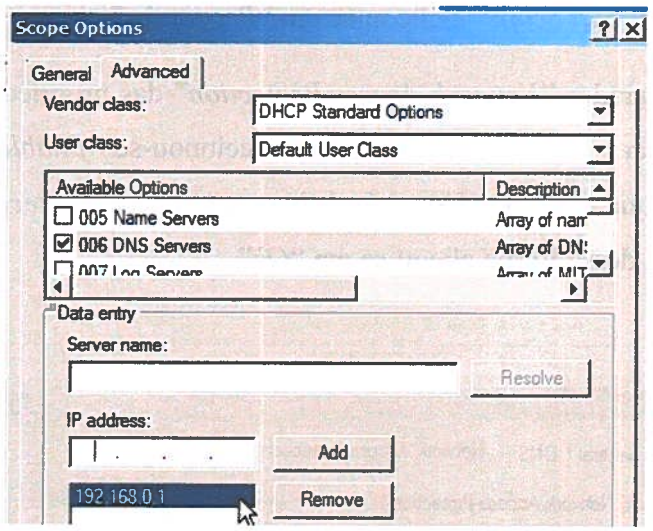

Figura 48 - Scope Options Default User Class 006 DNS Servers

Por fim, seleccionou-se a opção "*015 DNS Domain Name*" e em "*String Value*" introduziu-se "contoso.com" e clicou-se em "*Ok*". O domínio "contoso.com" permite o acesso completo da rede atribuído para clientes NAP que estão em conformidade.

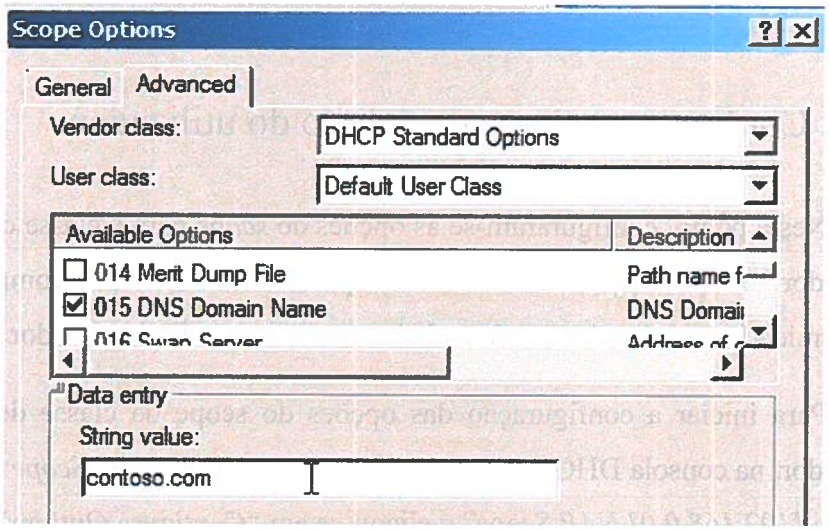

Figura 49 - Scope Options Default User Class 015 DNS Domain Name

7.6.3 Configurar a classe de defeito NAP

Neste ponto, configuraram-se as opções de *scope* para a classe de defeito NAP. Estas opções são utilizadas quando um cliente computador em inconformidade tenta aceder à rede e obtém um endereço IP do servidor DHCP.

Para iniciar a configuração das opções do scope da classe de defeito NAP, na consola DHCP clicou-se com o botão direito em "*Scope Options*" no "*Scope [192.168.0.0] NAP Scope*" e, assim, clicou-se em "*Configure Options*".

No separador "*Advanced*" do "*Scope Options*" em "*User class*" seleccionou-se "*Default Network Access Protection Class*". De seguida, seleccionou-se a opção "*006 DNS Servers*" e em "*IP Address*" introduziu-se 192.168.0.1 e, deste modo, clicou-se em "*Add*".

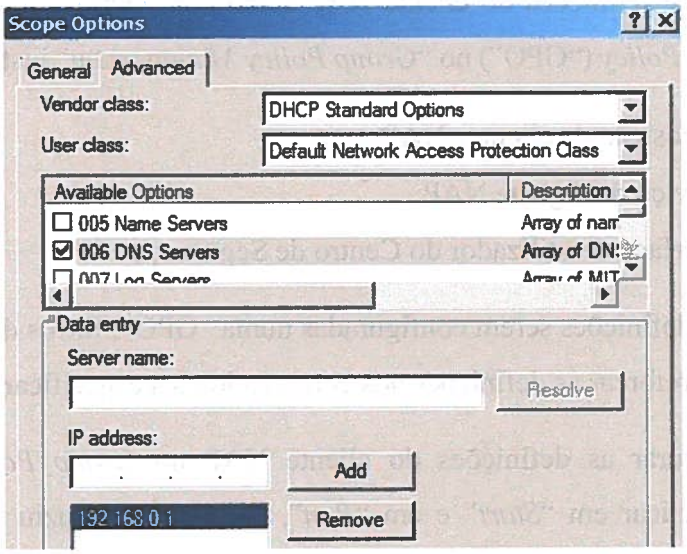

Figura 50 - Scope Options Default NAP Class 006 DNS Servers

Finalmente, seleccionou-se a opção "*015 DNS Domain Name*" e em "*String Value*" introduziu-se "restricted.contoso.com" e, assim, clicou-se em "*Ok*". O domínio "restricted.contoso.com" permite o acesso restrito da rede atribuído para clientes NAP que estão em inconformidade.

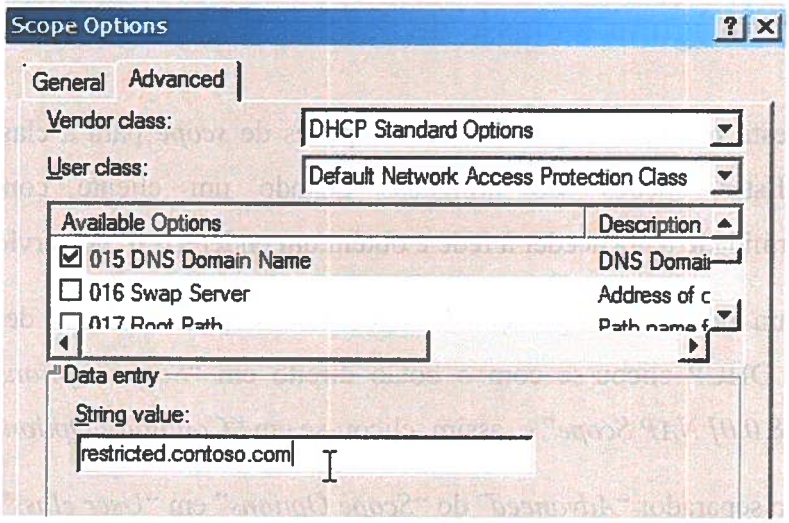

Figura 51 - Scope Options Default NAP Class 015 DNS Domain Name

7.7 Configurar as definições do cliente NAP no *Group Policy*

As seguintes definições do cliente NAP serão configuradas através de um novo objecto do *Group Policy* ("GPO") no "*Group Policy Management*" instalado no "NPS1":

- Imposição de clientes NAP;
- Serviço de Agente NAP;
- Interface de utilizador do Centro de Segurança.

Após estas definições serem configuradas numa "GPO", filtros de segurança serão adicionados para reforçar as definições nos computadores a especificar.

Para configurar as definições do cliente NAP no *Group Policy* no "NPS1", começou-se por clicar em "*Start*" e em "*Run*", onde se introduziu "*gpme.msc*" e de seguida pressionou-se em "ENTER".

Na janela "*Browse for a Group Policy Object*", clicou-se no ícone para criar uma nova GPO, sendo atribuído o nome "NAP Client Settings". Clicou-se em "*Ok*".

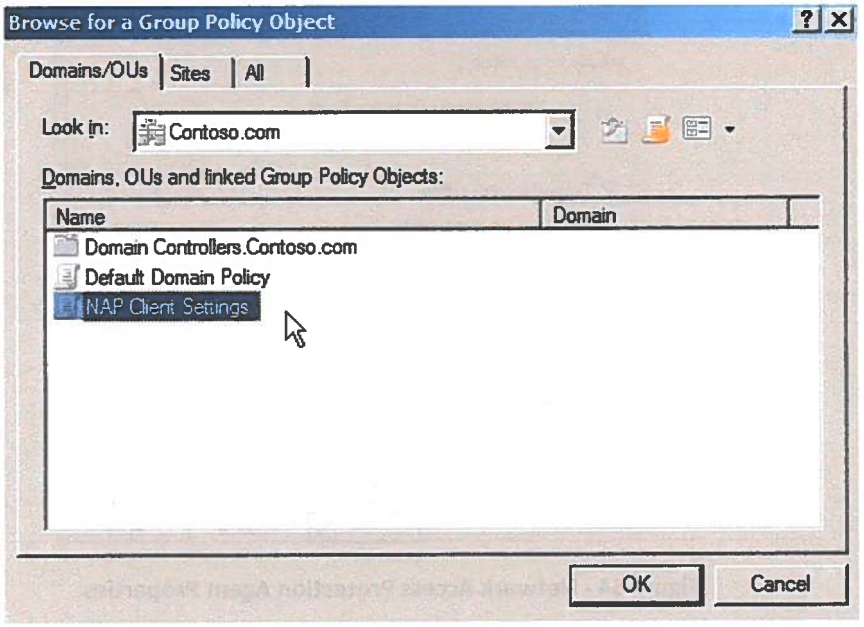

Figura 52 - NAP Client Settings GPO

Na janela "*Group Policy Management Editor*", foi necessário aceder a "*Computer Configuration/Policies/Windows Settings/Security Settings/System Services*".

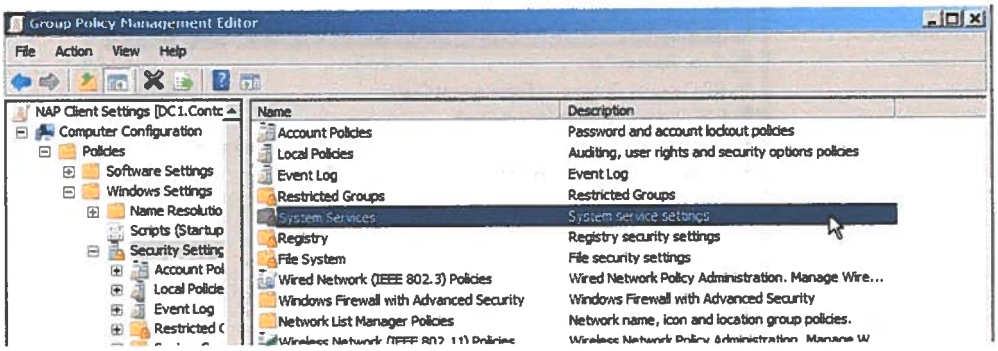

Figura 53 - System service settings

No painel de detalhes, efectuou-se duplo clique em "*Network Access Protection Agent*" e seleccionou-se "*Define this policy setting*". Deste modo, escolheu-se "*Automatic*" e clicou-se em "*Ok*".

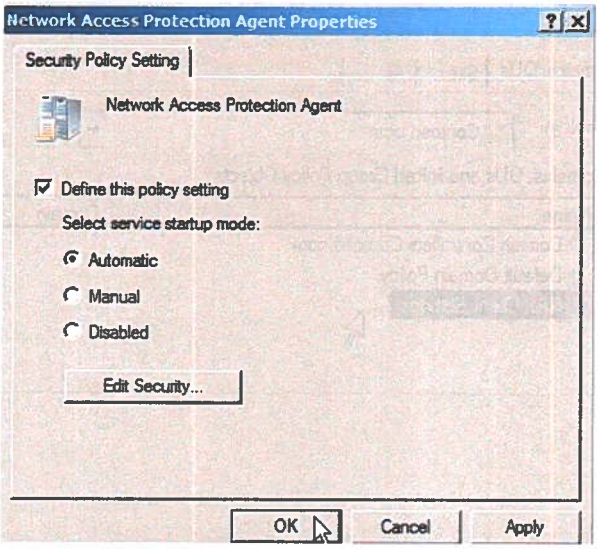

Figura 54 - Network Access Protection Agent Properties

Acedeu-se a "*Network Access Protection\NAP Client Configuration\Enforcement Clients*" e no painel de detalhes clicou-se com o botão direito em "*DHCP Quarantine Enforcement Client*" e posteriormente em "*Enable*".

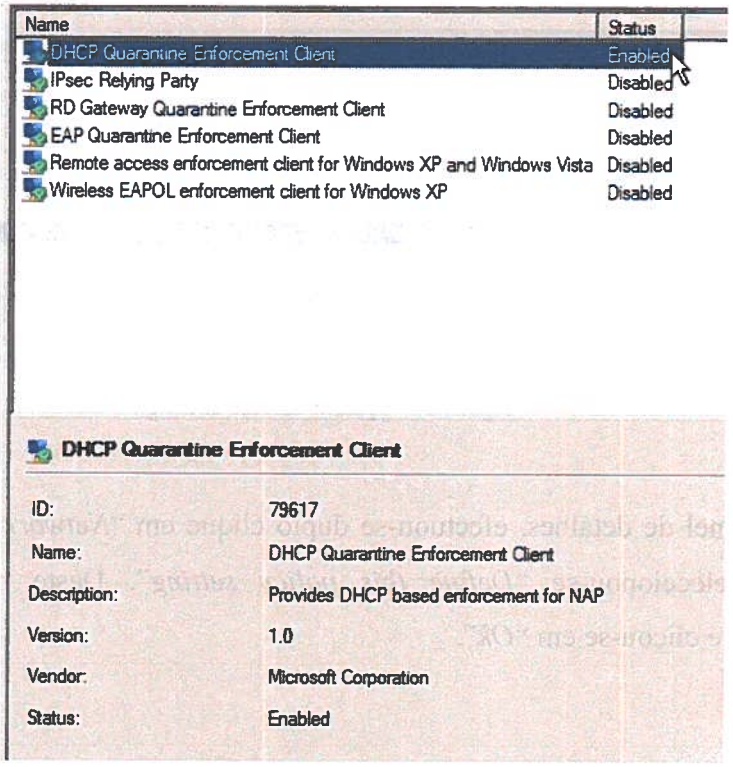

Figura 55 - DHCP Quarantine Enforcement Client

Em seguida, acedeu-se a "*Computer Configuration\Policies\Administrative Templates\Windows Componentes\Security Center*" e no painel de detalhes fez-se duplo clique em "*Turn on Security Center (Domain PCs only)*", seleccionou-se "*Enable*" e clicou-se em "*Ok*".

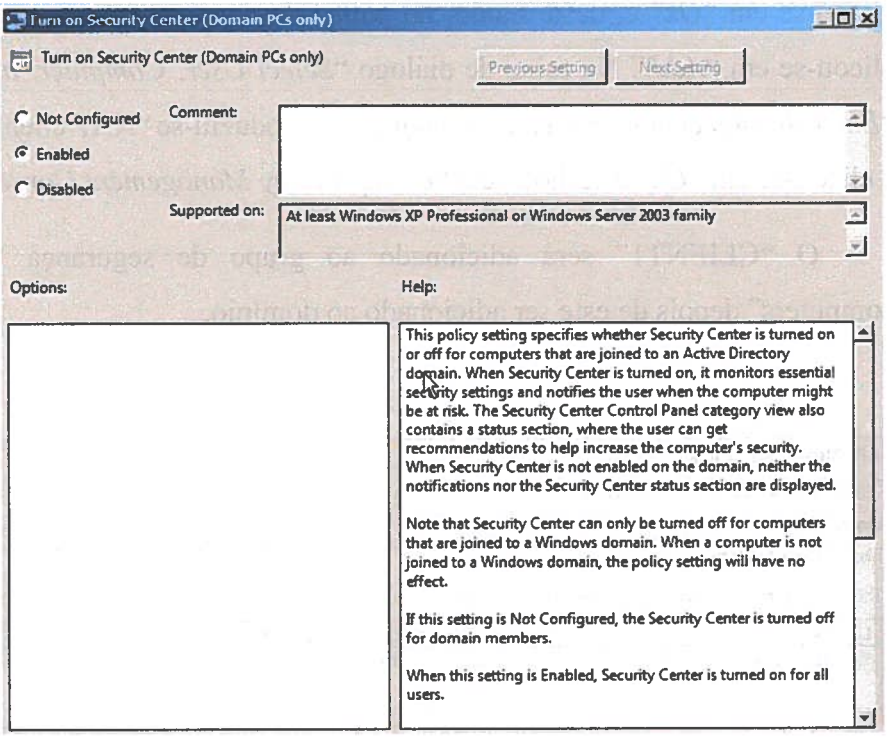

Figura 56 - Security Center

Fechou-se a janela do "*Group Policy Management Editor*" e clicou-se em "*Yes*" para aplicar as anteriores configurações.

7.7.1 Configurar filtros de segurança para as definições GPO do cliente NAP

Neste ponto, foram configurados os filtros de segurança para as definições GPO do cliente NAP. A aplicação destes filtros vai permitir que as definições do cliente NAP não sejam aplicadas a computadores servidores no domínio.

Para começar a configurar os filtros de segurança no "NPS1", clicou-se em "*Start*" e em "*Run*", onde se introduziu "*gpmc.msc*" e pressionou em "ENTER".

Em "*Group Policy Management Console*" acedeu-se a "*Forest: Contoso.com\Domains\Contoso.com\Group Policy Objects\NAP Client Settings*", em "*Security Filtering*" clicou-se em "*Authenticated Users*" e, de seguida, em "*Remove*".

Ao surgir uma caixa que confirma a remoção da delegação de privilégios, clicou-se em "*Ok*" e, deste modo, no painel de detalhes em "*Security Filtering*" clicou-se em "*Add*". Na caixa de diálogo "*Select User, Computer, or Group*" em "*Enter the object name to select (exemples)*" introduziu-se "NAP client computers", e clicou-se em "*Ok*" e fechou-se o "*Group Policy Management Console*".

O "CLIENT1" será adicionado ao grupo de segurança "NAP client computers" depois de este ser adicionado ao domínio.

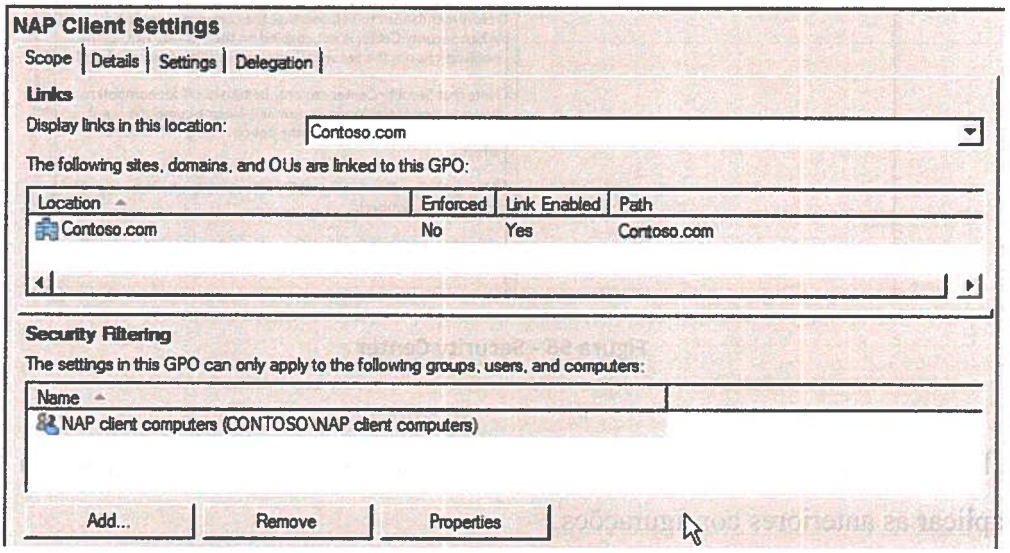

Figura 57 - GPO NAP Client Settings

Capítulo 8 – Configuração do CLIENT1

Neste capítulo, será abordada a configuração do cliente de nome "CLIENT1". Este, após a instalação do sistema operativo, vai servir como demonstração de como o NAP consegue ser usado com o DHCP para ajudar a proteger a rede de computadores clientes em inconformidade.

A configuração do "CLIENT1" consiste nos seguintes passos:

- Instalação do sistema operativo;
- Configuração TCP/IP;
- Verificar a conectividade da rede;
- Associar o computador ao domínio;
- Adicionar "CLIENT1" ao grupo de segurança "NAP client computers" e reiniciar o computador;
- Verificar as definições do *Group Policy*.

8.1 Configuração TCP/IP do DC1

Após instalação do sistema operativo é necessário configurar as definições TCP/IP do sistema.

À semelhança do capítulo 6.1, o método de configuração apenas difere na obtenção automática de um endereço de IP e de um endereço de servidor DNS.

8.2 Conectividade de teste para o CLIENT1

De momento o "CLIENT1" não está associado ao domínio, ainda não recebeu as definições do *Group Policy* para começar o serviço de Agente NAP. Quando o serviço Agente NAP não está a ser executado, o "CLIENT1" é considerado com um *"non-NAP-capable"*. Por defeito, o assistente de configuração NAP permite acesso restrito a clientes *"non-NAP-capable"*.

Executando o comando "ping" no "CLIENT1" confirmou-se a perda de conexão entre o "CLIENT1" e o "DC1".

Para executar o comando "ping" de modo a verificar a conectividade, clicou-se em "*Start*", posteriormente, em "*All Programs*" e depois em "*Accessories*". Fez-se um clique com o botão direito em "*Command Prompt*" e clicou-se em "*Run as administrator*".

Na janela de comando, introduziu-se "ping 192.168.0.1" e pressionou-se em "ENTER". Deste modo, a resposta obtida foi "*PING: transmit failed*".

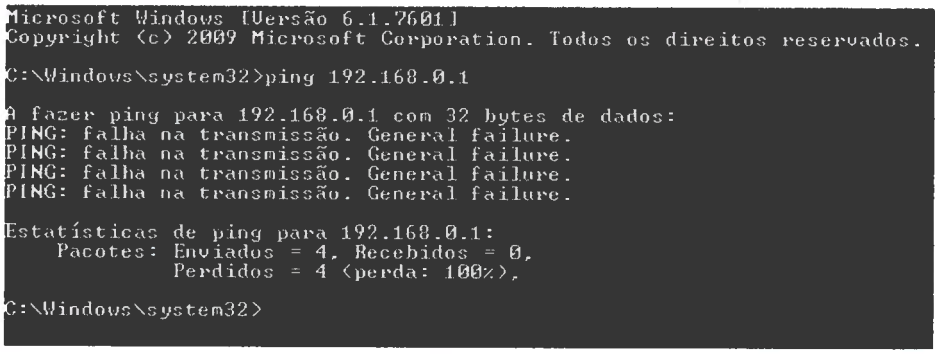

Figura 58 - Ping failed

Seguidamente, introduziu-se "ipconfig" e pressionou-se em "ENTER". Assim, verificou-se que o valor apresentado em "*Conection-specific DNS Suffix*" foi "restricted.contoso.com" e o valor da "*Subnet Mask*" foi "255.255.255.255". O "CLIENT1" foi configurado como um "classless network address", causando a restrição de acesso à rede.

Figura 59 - ipconfig

Ainda na janela de comando, introduziu-se "route print -4" e pressionou-se em "ENTER". A resposta deste comando permitiu verificar que o endereço 192.168.0.1 não foi exibido porque o "CLIENT1" tem um "classless network address", isto é, não tem uma rota activa para contactar o "DC1" e, como tal, não tem acesso aos serviços de domínio.

Por fim, verificou-se que 192.168.0.2 foi exibido no "*Network Destination*" em "*Active Routes*", este é o endereço IP do "NPS1" que serve como um servidor NAP de imposição DHCP.

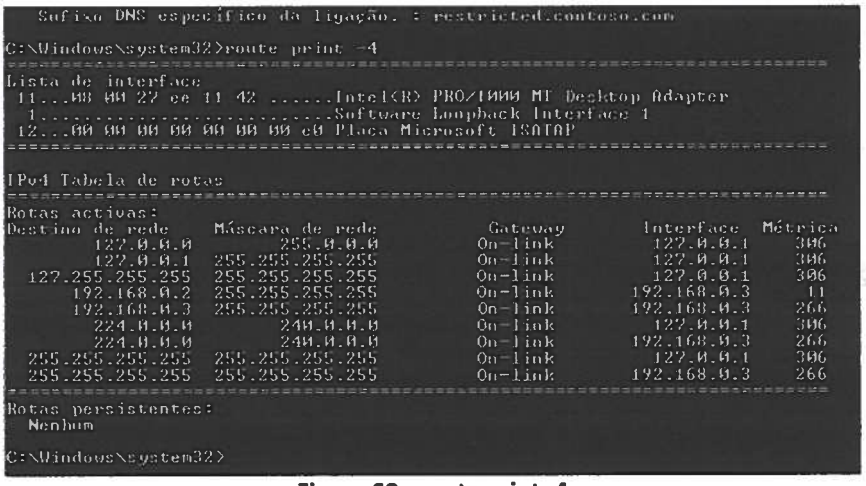

Figura 60 - route print -4

O servidor NAP de imposição DHCP está automaticamente disponível para clientes em rede restrita. Não será necessário adicionar este servidor para um grupo de servidor de remediação.

8.3 Configuração do DC1 como servidor de remediação

Neste ponto, configurou-se o "DC1" como um servidor de remediação para que o "CLIENT1" tenha acesso ao DNS e ao *Active Directory* quando este tiver acesso restrito.

Para começar a configuração, no "NPS1" clicou-se em "*Start*", em "*Run*" e introduziu-se "*nps.msc*". De seguida pressionou-se em "ENTER".

Na consola do "*Network Policy Server*", abriu-se a opção "*Policies*" e clicou-se em "*Network Policies*".

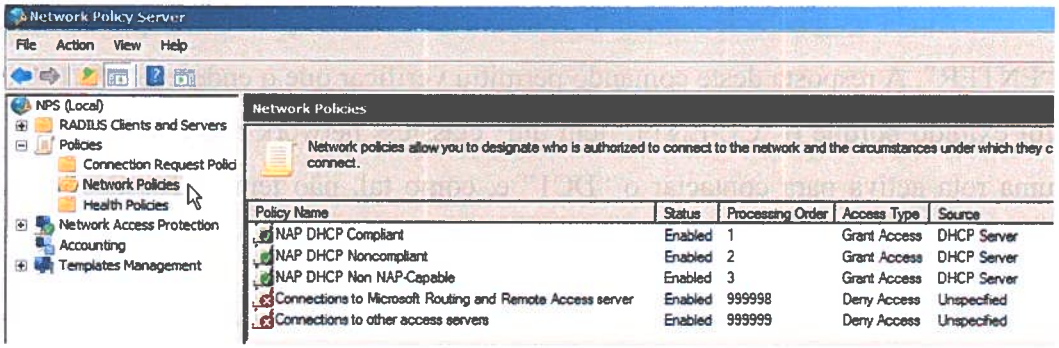

Figura 61 - Network Policies

No painel de detalhes fez-se duplo clique em "*NAP DHCP Non NAP-Capable*", no separador "*Settings*" clicou-se em "*NAP Enforcement*" e em "*Remediaton Server Group and Troubleshooting URL*" clicou-se em "*Configure*".

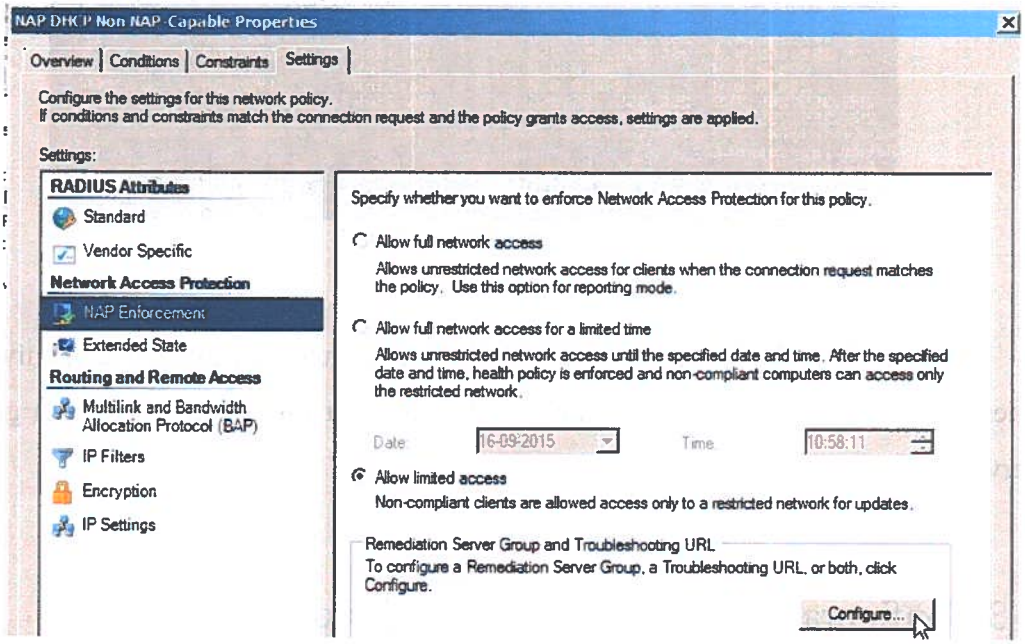

Figura 62 - NAP Enforcement Settings

Na caixa de diálogo "*Remediation Servers and Troubleshooting URL*", na opção "*Remediation Server Group*" clicou-se em "*New Group*". Na caixa de diálogo seguinte, em "*Group Name*" introduziu-se "Domain services" e clicou-se em "*Add*".

Na caixa de diálogo "*Add New Server*" em "*Friendly name*" introduziu-se "DC1", assim como em "*IP address or DNS name*" introduziu-se 192.168.0.1 e, desta forma, clicou-se em "Ok" duas vezes para finalizar.

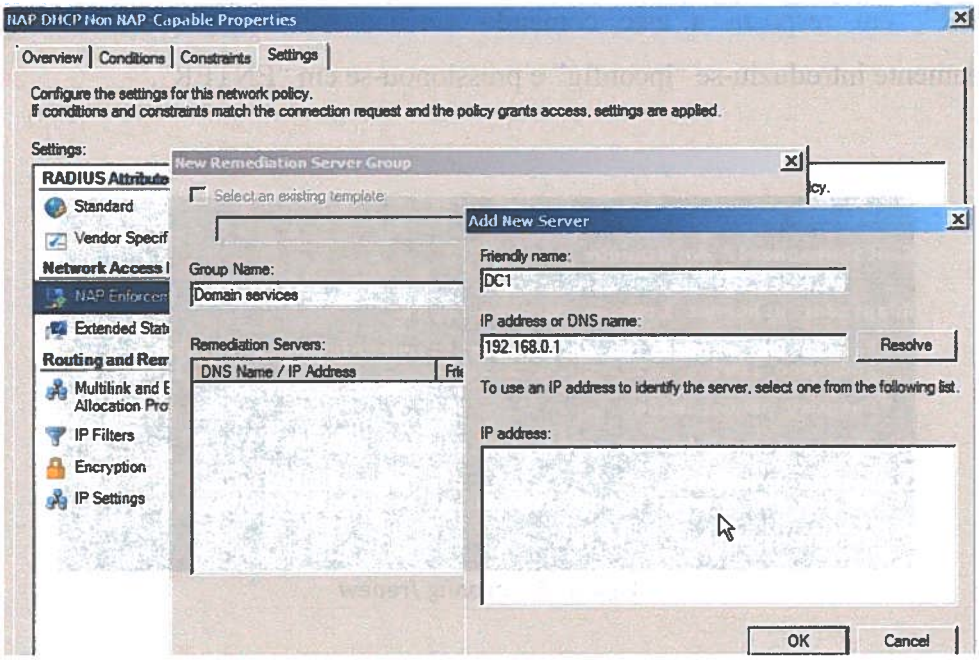

Figura 63 - New Remediation Server Group

Verificamos que um novo grupo de servidor de remediação foi seleccionado em "*Remediation Server Group*" e assim clicou-se em "*Ok*" para fechar a caixa de diálogo "*Remediation Servers and Troubleshooting URL*". Por fim, clicou-se em "*Ok*" para fechar a janela "*NAP DHCP Non NAP-Capable Properties*".

No painel de detalhes fez-se duplo clique em "*NAP DHCP Noncompliant*" e no separador "*Settings*", em "*Remediation Server Group and Troubleshooting URL*", clicou-se em "*Configure*". Seleccionou-se "*Domain services*" e clicou-se em "*Ok*" duas vezes para finalizar. O "DC1" ficou assim disponível como um servidor de remediação para os "non-NAP-capable and noncompliant" computadores.

8.4 Renovação de endereçamento de IP no CLIENT1

Seguidamente, pretende-se obter um novo perfil de endereço de IP para o "CLIENT1" através do DHCP.

Para começar a renovação de endereçamento no "CLIENT1", na janela "*Administrator: Command Prompt*" introduziu-se "ipconfig /renew" e pressionou-se em "ENTER". Na janela de comando introduziu-se "ping 192.168.0.1" e pressionou-se em

"ENTER", em resposta a este comando verificou-se "*Reply from 192.168.0.1*". Seguidamente introduziu-se "ipconfig" e pressionou-se em "ENTER".

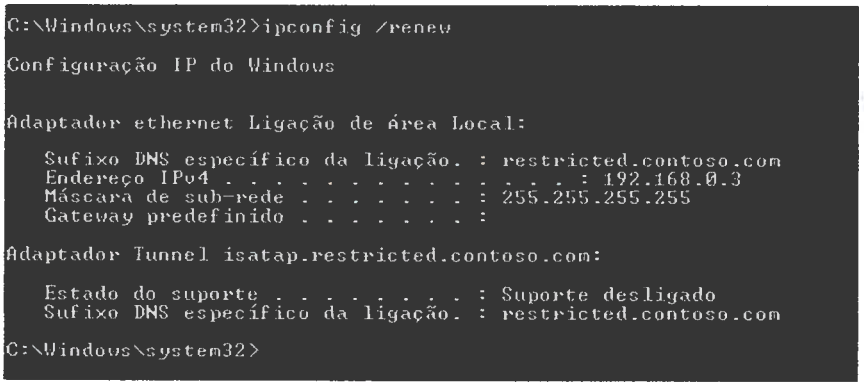

Figura 64 - ipconfig /renew

A resposta gerada ao comando "ipconfig" permitiu visualizar que o valor do "*Connection-specific DNS Suffix*" foi "restricted.contoso.com" e o valor da "*Subnet Mask*" foi 255.255.255.255. Estes valores devem se ao facto do serviço "*NAP Agent*" não estar em execução de momento no "CLIENT1", o acesso restrito à rede continua implementado.

Ainda na janela de comando, introduziu-se "route print -4" e pressionou-se em "ENTER". A resposta gerada permitiu que nas "*Active Routes*" o endereço 192.168.0.1 fosse exibido em "*Network Destination*". Isto porque o "DC1" é um membro do grupo dos servidores de remediação, ao "CLIENT1" foi garantido o acesso aos serviços de domínio na rede restrita.

Capítulo 9 – Verificação da funcionalidade NAP

Este capítulo tem como objectivo a verificação do correcto funcionamento na infra-estrutura NAP implementada. Deste modo, e para efeitos de demonstração, foram efectuados os seguintes procedimentos:

- Verificação de auto-remediação NAP: o "CLIENT1" é automaticamente remediado quando a *Windows Firewall* é desligada, o que causará a ligação da mesma;
- Verificação da política de imposição NAP: esta política será revista para ser mais restrita, o que causará a colocação do "CLIENT1" em estado de inconformidade com as políticas implementadas e, ainda, a não remediação do mesmo.

9.1 Verificação de remediação automática NAP

A política de rede "NAP DHCP noncompliant" determina que os computadores que se encontrem em estado de inconformidade devem ser automaticamente remediados para um estado de conformidade, quando a *Windows Firewall* é desligada.

Para começar a verificação de auto-remediação do "CLIENT1", quando a *Windows Firewall* é desligada, acedeu-se ao painel de controlo do "DC1" e, no "*Security Center*", clicou-se em "*Windows Firewall*".

Nas opções do "*Windows Firewall*" clicou-se em "*Off (not recommended)*" e posteriormente em "*Ok*".

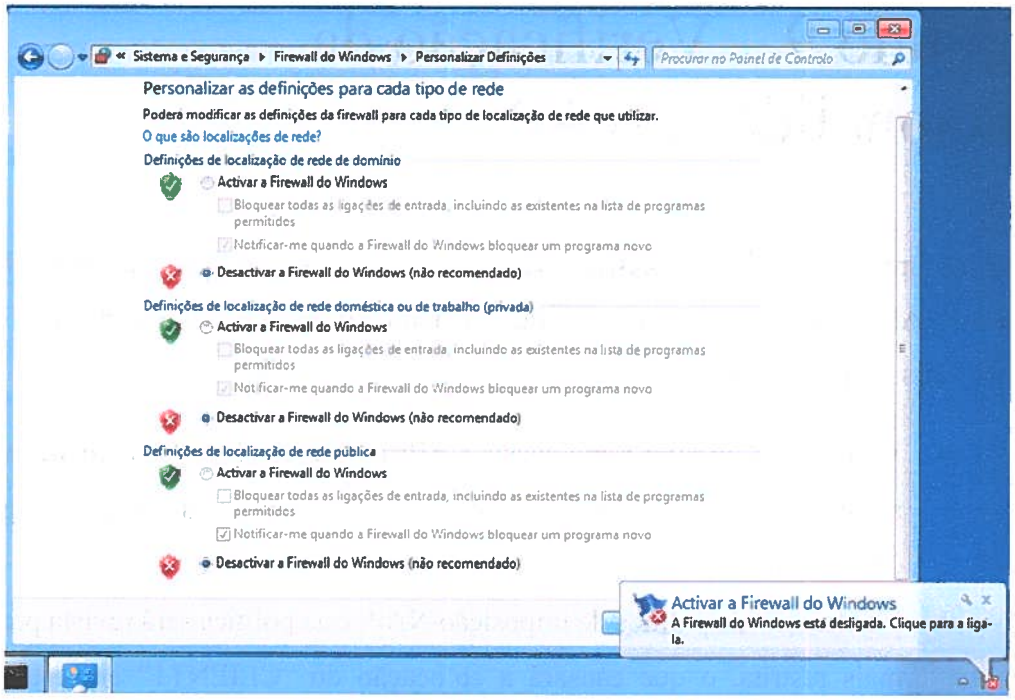

Figura 70 - Windows Firewall desligada

Verificou-se que no "*Windows Security Center*" a *Windows Firewall* foi desactivada e que momentos depois foi activada.

Verificou-se, também, que na área de notificações foi exibida uma mensagem a indicar que o computador não reúne os requisitos de integridade necessários. Esta mensagem foi exibida porque a *Windows Firewall* foi desligada.

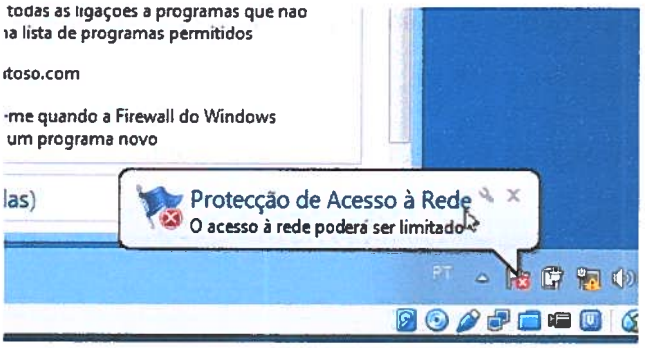

Figura 71 - Protecção de Acesso à Rede

O cliente NAP vai ligar automaticamente a *Windows Firewall* e este vai ficar em conformidade com os requisitos de integridade da rede. Deste modo, foi exibido uma mensagem na área de notificações a confirmar o acesso completo à rede.

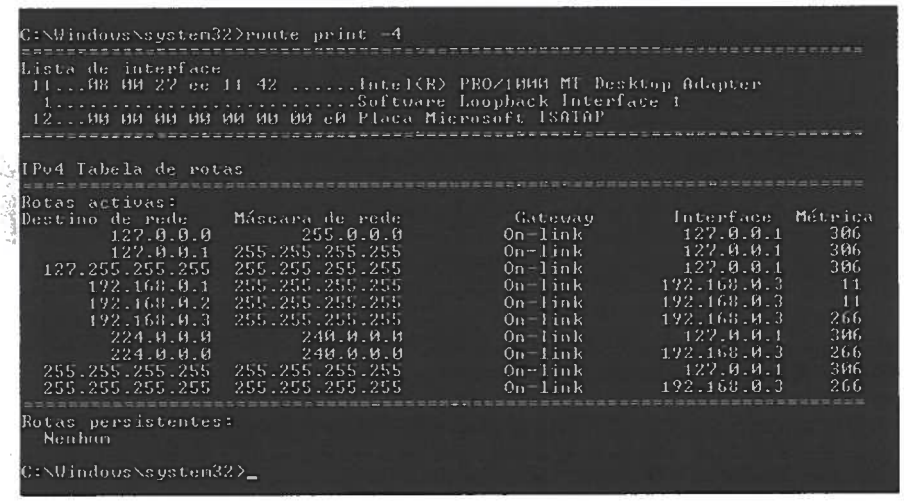

Figura 65 - route print -4

8.5 Associar CLIENT1 ao domínio "Contoso.com"

Como o "CLIENT1" agora tem acesso a serviços do domínio é possível associa-lo.

Para associar o "CLIENT1" ao domínio "Contoso.com" acedeu-se às propriedades do sistema, onde se introduziu "Contoso.com" na opção "*Domain*" e seleccionou-se "*Primary DNS suffix of this computer*" na opção "*More*". Quando solicitada informação de aceso para confirmar a configuração, introduziram-se os dados da conta do utilizador "User1". Antes de reiniciar, para aplicar as alterações, foi necessário adicionar o "CLIENT1" ao grupo de segurança dos computadores clientes NAP para que receba as definições NAP do *Group Policy*.

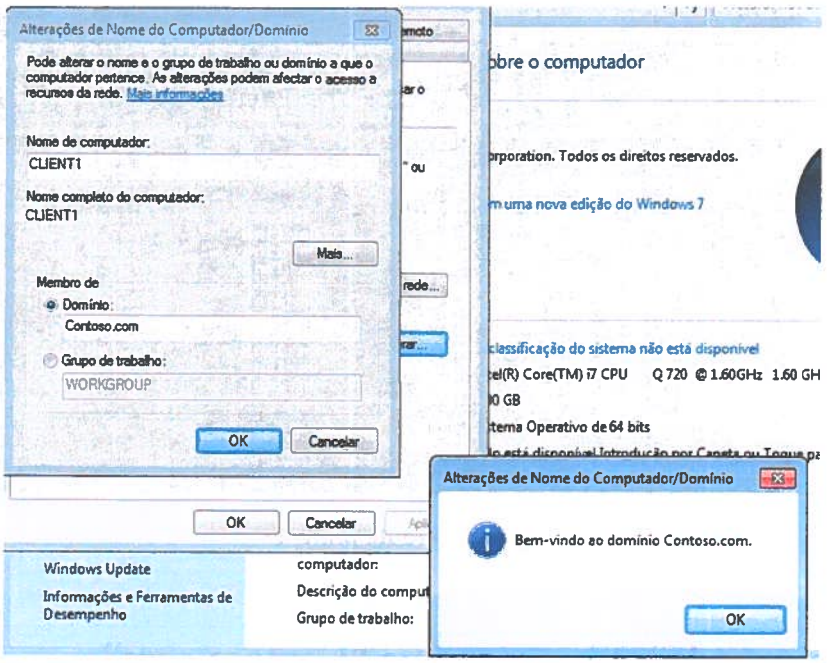

Figura 66 - Contoso.com

8.6 Adicionar o CLIENT1 ao grupo de segurança dos computadores clientes NAP

Para adicionar o "CLIENT1" ao grupo de segurança, acedeu-se ao "*Active Directory Users and Computers*" do "DC1".

Em "Contoso.com", acedeu-se às propriedades do grupo de segurança *"NAP client computers"* e no separador "*Members*" clicou-se em "*Add*". Na caixa de diálogo seguinte, seleccionou-se a opção "*Computers*" e adicionou-se "CLIENT1". Assim, verificou-se que "CLIENT1" foi exibido em "*Members*".

Por fim, reiniciou-se o "CLIENT1" para aplicar o novo membro do grupo de segurança.

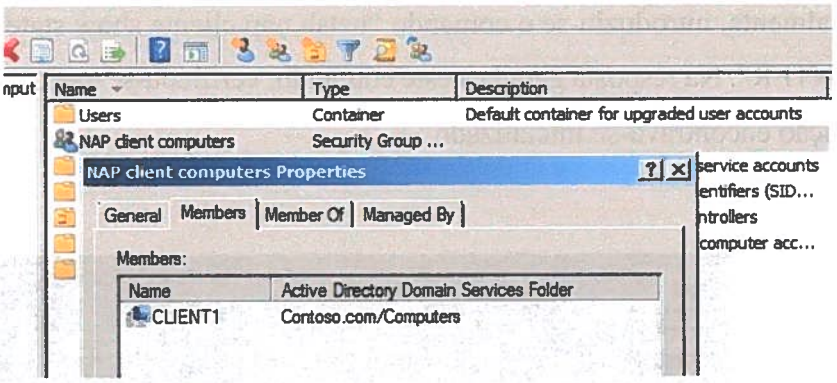

Figura 67 - CLIENT1 membership

8.7 Verificar as definições do *Group Policy*

Após reiniciar o "CLIENT1", este irá receber as definições do *Group Policy,* de modo a que o serviço "*NAP Agent*" fique disponível, assim como, a imposição do método DHCP ao cliente.

Para verificar as definições do *Group Policy* no "CLIENT1" acedeu-se à janela de comando, introduziu-se "netsh nap cliente show grouppolicy" e pressionou-se em "ENTER". Na resposta gerada a este comando, verificou-se que em "*Enforcement clients*" o estado de "*Admin*" se encontrava activado em "*DHCP Quarantine Enforcement Client*".

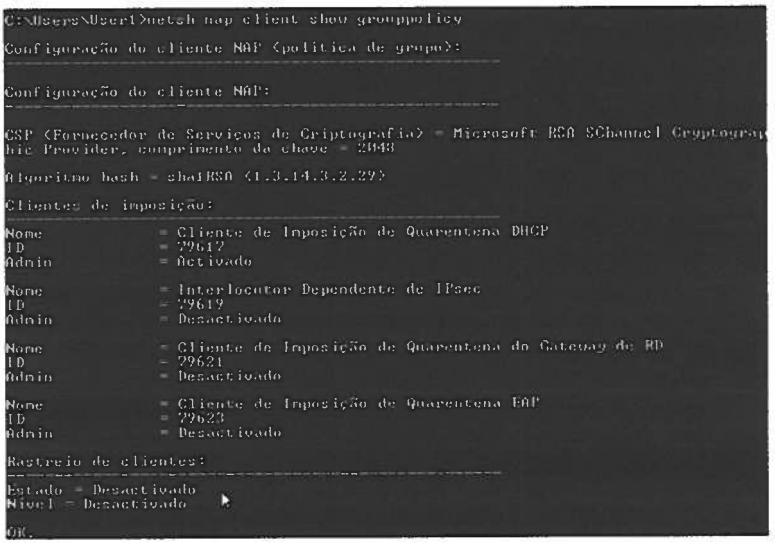

Figura 68 - DHCP Quarantine Enforcement Client

Finalmente, introduziu-se o comando "netsh nap cliente show state" e pressionou-se em "ENTER". Na resposta gerada a este comando, verificou-se que o estado do cliente de imposição encontrava-se inicializado.

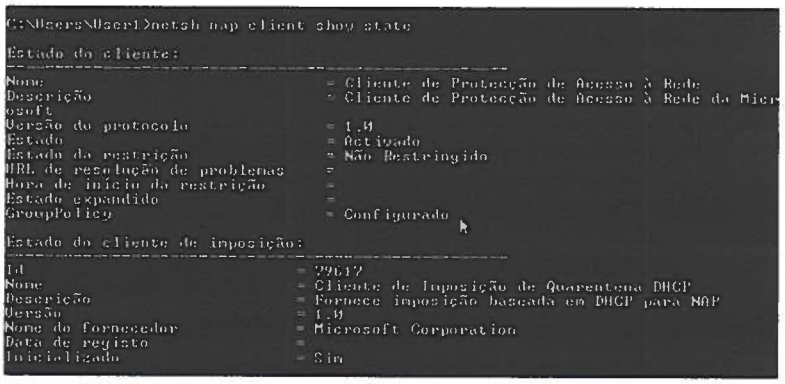

Figura 69 - DHCP Quarantine Enforcement Client

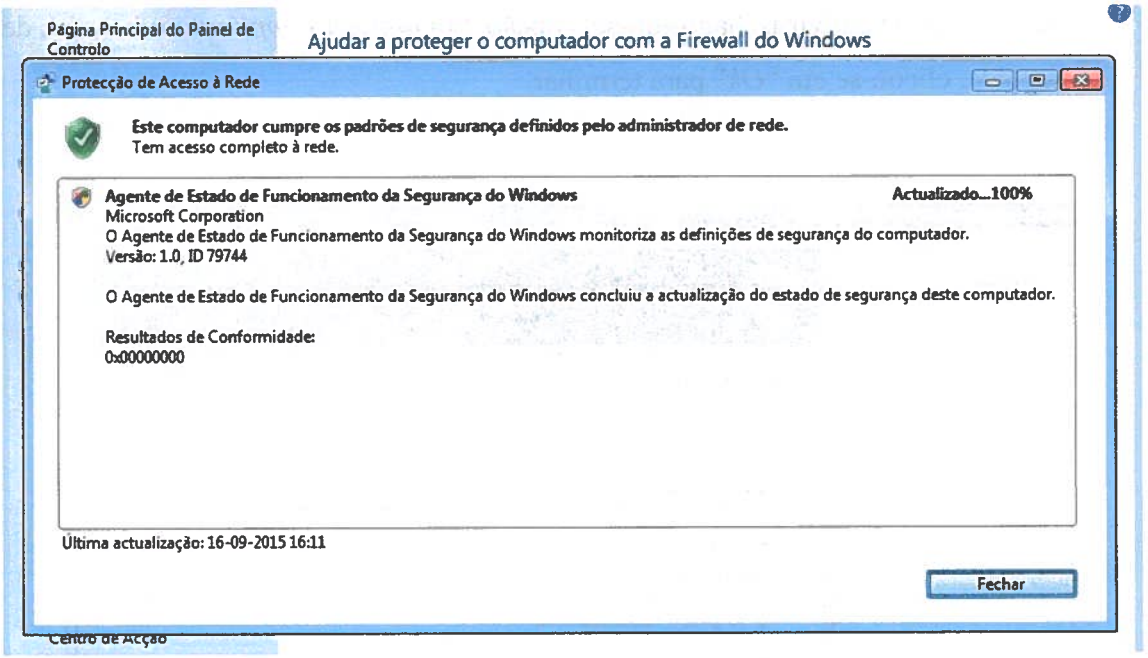

Figura 72 - Protecção de Acesso à Rede

9.2 Verificação da política de imposição NAP

A política de imposição de rede será verificada na configuração de um requisito adicional à política de rede. Este não será cumprido pelo "CLIENT1" e, como consequência, será colocado na rede restrita.

9.2.1 Configuração de WSHV para requer uma aplicação antivírus

Será efectuada uma configuração no "NPS1" para que um *software* antivírus seja necessário, de modo a cumprir com os padrões de segurança definidos no sistema.

O "CLIENT1" será considerado como estando em estado de inconformidade, porque não foi instalado um programa antivírus no "CLIENT1", e os componentes de cliente NAP não conseguem remediar o seu estado.

Para começar a configuração, abriu-se a consola "*Network Policy Server*" do "NPS1", onde se acedeu às propriedades de "*Windows Security Health Validator*".

Nas opções de antivírus, habilitou-se a opção "*An antivirus application is on*" e, de seguida, clicou-se em "*Ok*" para terminar.

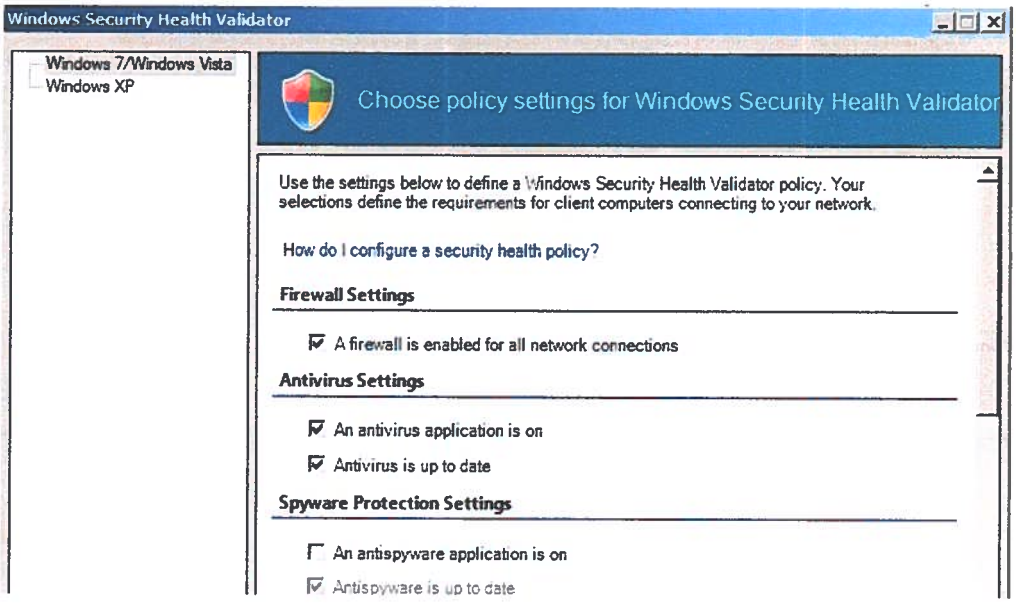

Figura 73 - WSHV Antivirus Settings

9.2.2 Liberar ("release") e renovar ("renew") o endereço de IP no CLIENT1

Para revalidar o estado de integridade do "CLIENT1", contra novos requisitos de integridade da rede, desligou-se a *Windows Firewall.* Deste modo, seria previsto que o "CLIENT1" remediasse, automaticamente, a configuração da *Windows Firewall.* No entanto, como não foi efectuada a instalação de um antivírus, não foi possível remediar esta situação. Desta forma, o "CLIENT1" continuou em estado de inconformidade e obteve uma configuração de endereço de IP para a rede restrita.

Nas configurações da *Windows Firewall* do "CLIENT1", clicou-se em "*Off (not recommended)*" e em "*Ok*". Deste modo, no "*Windows Security Center*", verificou-se que a *Windows Firewall* inicialmente estava desligada e que posteriormente ficou ligada. Apesar de a *Windows Firewall* estar ligada, o "CLIENT1" não consegue instalar uma aplicação antivírus automaticamente, assim, o mesmo manterá o seu estado de inconformidade e o acesso à rede limitado.

9.2.3 Estado de restrição do cliente

Considerando o computador cliente em estado de inconformidade, o servidor DHCP irá atribuir ao mesmo um endereço de IP para a rede restrita. Assim, será possível identificar que o cliente se encontra na rede restrita porque o servidor DHCP atribuiu, em "*Connection-specific DNS suffix*", o valor de "restricted.contoso.com", como na figura seguinte é demonstrado:

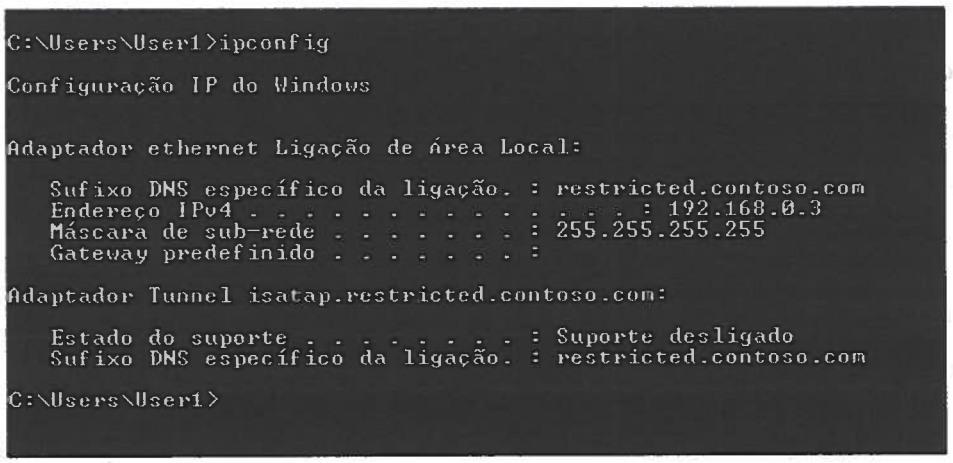

Figura 74 - Restrição do cliente

Foi possível verificar o estado de restrição do computador usando o comando NAP Netsh.

Introduziu-se "*netsh nap cliente show state*" na janela de comando e pressionou-se em "ENTER". A resposta gerada permitiu verificar que o estado do cliente se encontrava restrito, como ilustra a seguinte imagem.

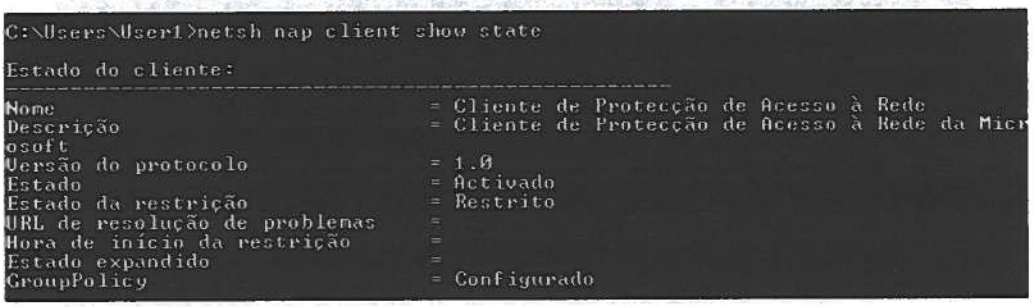

Figura 75 - Estado de restrição do cliente

9.2.4 Permitir a conformidade ao CLIENT1

Neste ponto, foi efectuada a configuração do "NPS1" para remover o requisito de integridade de antivírus, de modo a que o "CLIENT1" seja considerado como estando no estado de conformidade. Para tal, foi necessário usar o comando "ipconfig" para liberar e renovar o endereço de IP no "CLIENT1" e, assim, gerar um novo SoH.

Para inicializar a configuração no "NPS1", abriu-se a consola "*Network Policy*" e, nas propriedades do "*Windows Security Validator*", clicou-se em "*Configure*". Posteriormente, nas opções de antivírus retirou-se o visto da opção "*An antivirus application is on*" e clicou-se em "*Ok*" duas vezes para confirmar a configuração do WSHV.

No "CLIENT1", introduziu-se "ipconfig /release" e "ipconfig /renew", na janela de comandos, de modo a obter uma nova configuração de endereço IP com acesso completo.

Na resposta gerada a estes comandos, verificou-se que uma nova configuração de endereço de IP foi atribuída. Isto confirmar-se pois o sufixo DNS específico da ligação passou a ser "contoso.com".

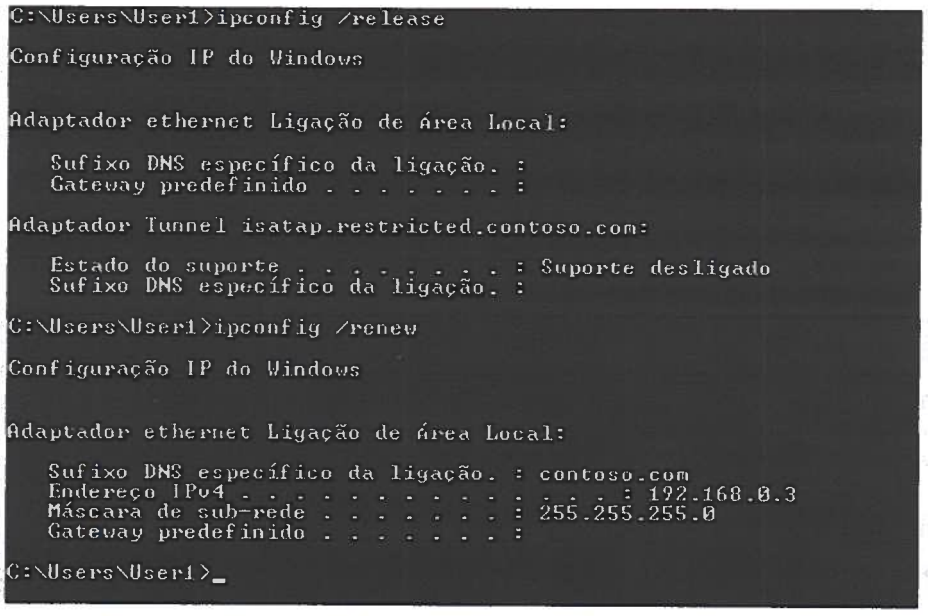

Figura 76 - CLIENT1 em conformidade

Capítulo 10 – Conclusão

Os administradores de redes enfrentam o desafio do consumo de tempo ao garantir a segurança dos computadores que se conectam a uma rede privada e que estes cumpram com as exigências das políticas de segurança da rede em que se encontram. A falta de monitorização e manutenção dos computadores conectados à rede põe em risco a sua integridade.

Em resposta a este desafio, o NAP surgiu para responder às necessidades dos administradores de redes como uma ferramenta de fácil implementação. Permite detectar e monitorizar ameaças, estabelece padrões de segurança e garante que sejam cumpridas as políticas estabelecidas. Possibilita, ainda, manter a rede resiliente, corrige vulnerabilidades e gerencia as políticas de segurança e o sistema de remediação. Deste modo, constata-se que o NAP surgiu, no sistema operativo Windows Server 2008, como uma ferramenta indispensável no que diz respeito à segurança das redes informáticas.

Em conclusão, no âmbito deste projecto, constata-se que é essencial, nos tempos que correm, o uso de tecnologias que permitem garantir a segurança das redes informáticas. Deste modo, ferramentas como o NAP são uma mais-valia neste sentido pois possibilitam um alerta permanente para os administradores de redes. No âmbito da componente prática deste projecto, verificou-se a possibilidade de implementação do *Network Access Protection* de forma intuitiva e recorrendo a tecnologias de virtualização de sistemas. No que diz respeito ao objectivo do projecto, este foi atingido e verificou-se o correcto funcionamento do *Network Access Protection.*

Referências

How Windows PowerShell Works. (n.d.). Retrieved from Microsoft Web Developer: http://msdn.microsoft.com/en-us/library/ms714658(v=vs.85).aspx

Hughes, L. (1995). *Actually Usefull Internet Security Techniques*. CA, USA: New Riders Publishing Thousands Oaks.

Hyper-V Getting Started Guide. (n.d.). Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc732470(v=WS.10).aspx

Internet Explorer. (s.d.). Obtido de Microsoft: http://windows.microsoft.com/pt-pt/internet-explorer/download-ie

Kizza, J. M. (2009). *Guide to Computer Network Security*. London: Springer.

Lucas, M. (2013, Janeiro 20). Retrieved from Microsoft TechNet Blogs: http://blogs.technet.com/b/askpfeplat/archive/2013/01/02/windows-server-2012-does-refs-replace-ntfs-when-should-i-use-it.aspx

Microsoft. (Fevereiro de 2008). *Microsoft Introduction to Network Access Protection White Paper*. Obtido de Microsoft.com: https://technet.microsoft.com/en-us/network/cc984252.aspx

Microsoft. (Novembro de 2008). *Microsoft Network Access Protection Deployment Guide*. Obtido de Microsoft.com: https://technet.microsoft.com/library/dd314175.aspx

Microsoft. (Outubro de 2008). *Microsoft Network Access Protection Design Guide*. Obtido de Microsoft.com: https://msdn.microsoft.com/en-us/library/dd125338(v=ws.10).aspx

Microsoft. (Fevereiro de 2008). *Microsoft Step By Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab*. Obtido de Microsoft.com: https://www.microsoft.com/en-us/download/details.aspx%3Fid%3D2409+&cd=1&hl=pt-PT&ct=clnk&gl=pt

Natário, R. (2011). *Alta disponibilidade - Terminologia (II)*. Obtido de Redes & Servidores: http://redes-e-servidores.blogspot.pt/2011/02/disponibilidade-terminologia-ii.html#cluster

Natário, R. (2011). *Balanceamento de Carga (I)*. Obtido de Redes e Servidores: http://redes-e-servidores.blogspot.pt/2011/03/balanceamento-de-carga-i.html

Natário, R. (2011). *Balanceamento de Carga (V)*. Obtido de Redes & Servidores: http://redes-e-servidores.blogspot.pt/2011/04/balanceamento-de-carga-v.html

Natário, R. (2011). *Failover Clustering (I)*. Obtido de Redes e Servidores: http://redes-e-servidores.blogspot.pt/2011/04/failover-clustering-i.html

Network Policy and Access Services. (n.d.). Retrieved from Microsoft Technet: https://technet.microsoft.com/en-us/network/bb545879.aspx

Ondrusek, J. (2010, Maio). *Server Core Installation Option of Windows Server 2008 and Windows Server 2008 R2 Getting Started Guide*. Retrieved from Microsoft Server 2008.

Self-Healing NTFS. (n.d.). Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc771388(v=ws.10).aspx

Server Manager. (2008, Janeiro 21). Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc732131(v=WS.10).aspx

Server Manager Step-by-Step Guide: Scenarios. (2008, Janeiro 21). Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc753762%28v=ws.10%29.aspx

Server Roles and Technologies in Windows Server 2012 R2 and Windows Server 2012. (2012, Fevereiro 29). Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/library/hh831669.aspx

What Is an RODC. (2012, Abril 26). Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc771030%28v=ws.10%29.aspx

Windows BitLocker™ Drive Encryption Step by Step Guide. (s.d.). Obtido de Microsoft: http://go.microsoft.com/fwlink/?LinkId=53779

Windows Firewall. (n.d.). Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/network/bb545423.aspx

Windows Server Backup Step-by-Step Guide for Windows Server 2008. (2013, Janeiro 17). Retrieved from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc770266%28v=ws.10%29.aspx