Sessão 9: Configuração segura de servidores Windows

1) Configuração do controlador de domínio *Active Directory*

Esta atividade será realizada na máquina virtual *WinServer-G*.

Nesta atividade iremos instalar e configurar a *role Active Directory* na máquina *WinServer-G*, tornando-o um controlador de domínio primário (também conhecido como AD DC — *Active Directory Domain Controller*) para o domínio `domainG.esr.local`, sendo `G` a letra associada ao seu grupo. Para fazer isso, siga os passos abaixo:

1. Acesse a máquina *WinServer-G* como o usuário `Administrator`. Acesse *Start* > *Run...* e digite `dcpromo.exe`. Clique em *OK*. O Windows Server irá iniciar o processo de instalação dos binários do *Active Directory* na máquina e, ao final do processo, irá abrir o *wizard* de configuração como se segue:

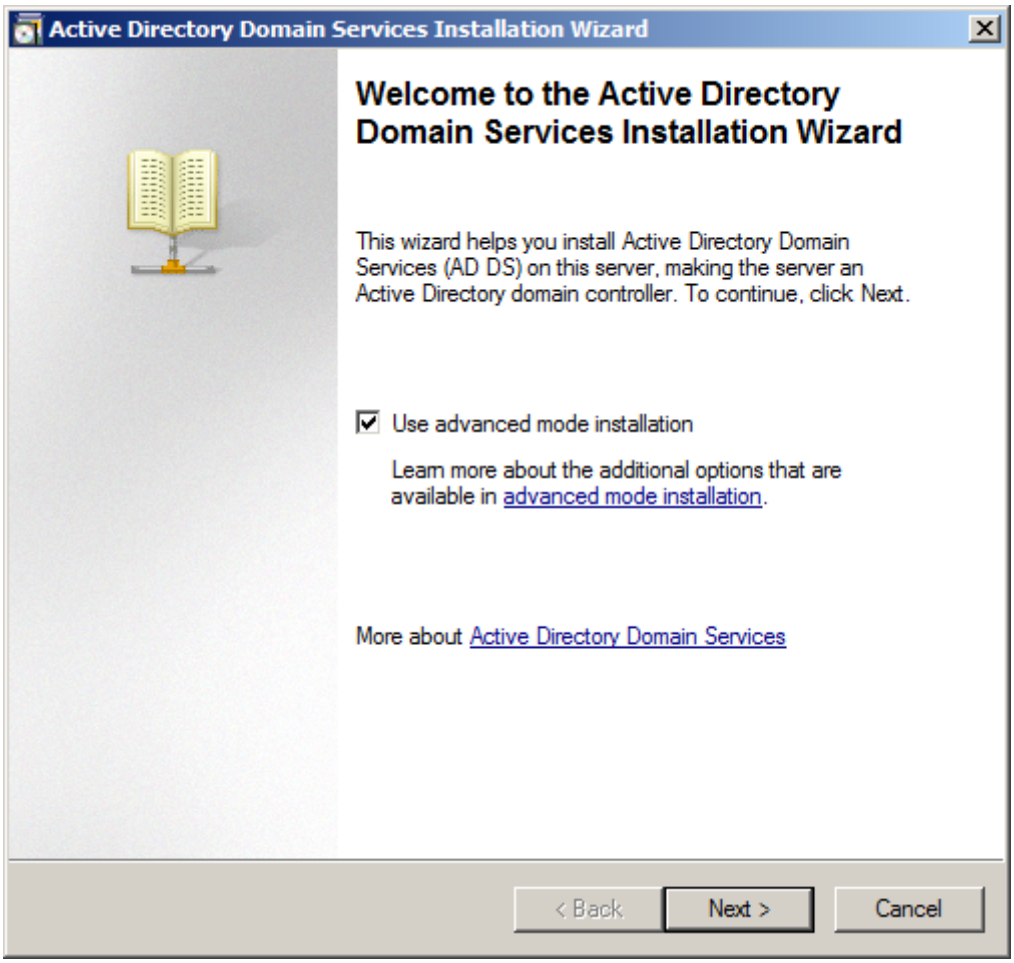

Figura 76: Tela inicial de configuração do AD DC

   Marque a opção *Use advanced mode installation* e clique em *Next*.

2. Na tela *Operating System Compatibility*, clique em *Next*.

3. Na tela *Choose a Deployment Configuration*, selecione *Create a new domain in a new forest*, como mostrado abaixo, e clique em *Next*.

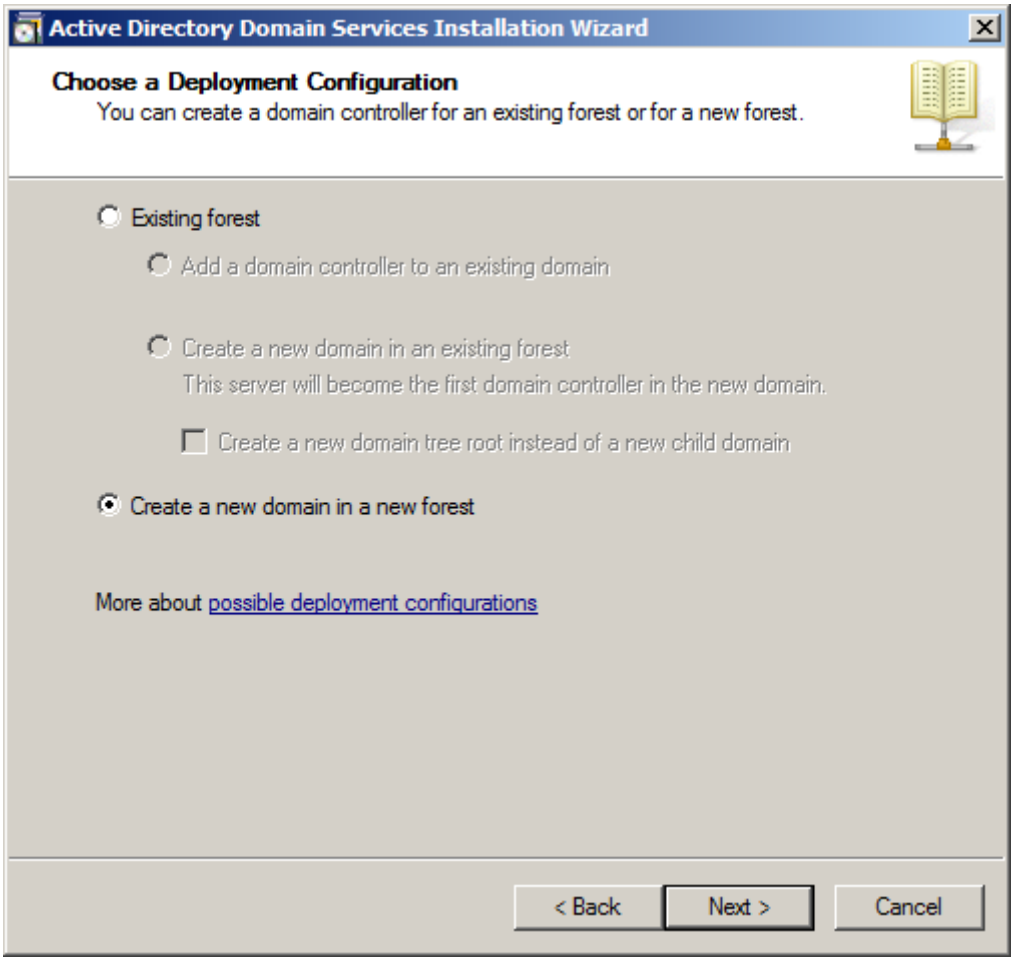

Figura 77: Escolha de tipo de instalação do AD DC

4. Na tela *Name the Forest Root Domain*, escolha o FQDN do seu domínio. Se estiver no grupo A, digite `domainA.esr.local`; no grupo B, digite `domainB.esr.local`. Verifique sua entrada de acordo com a imagem que se segue, e clique em *Next*.

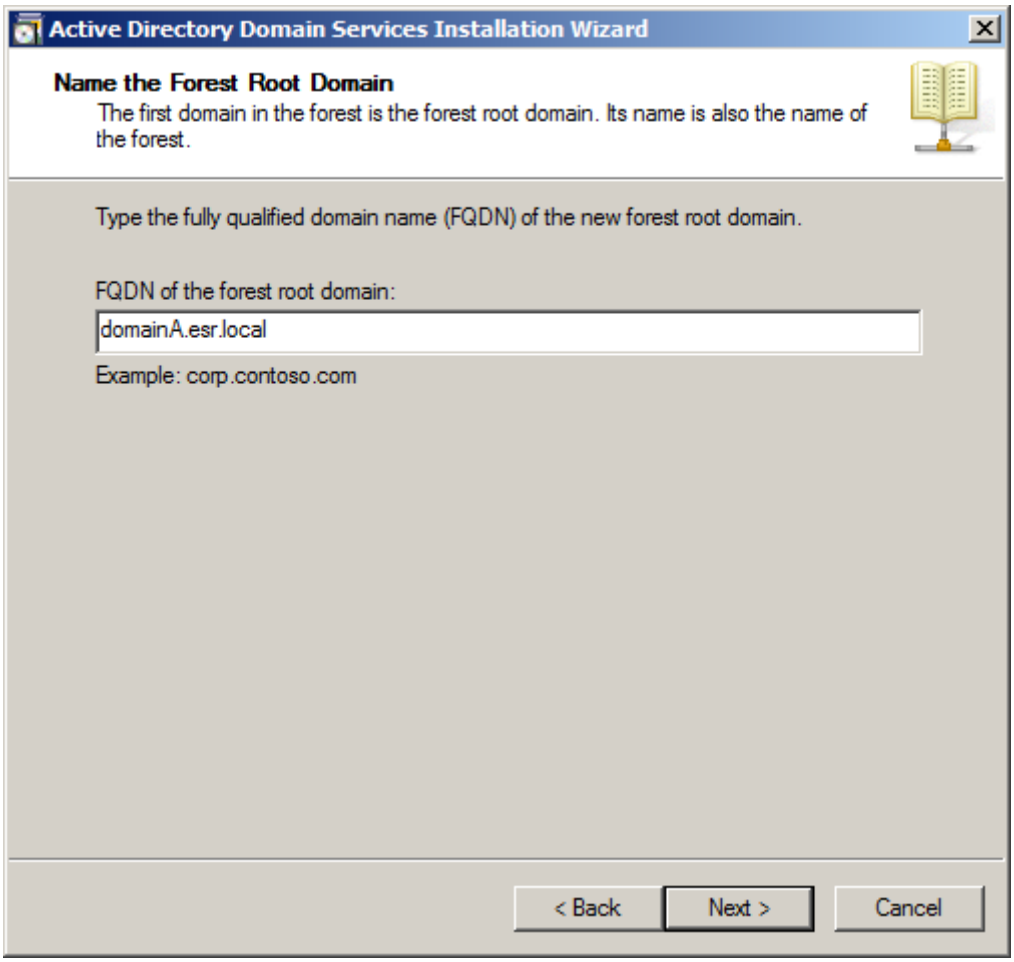

Figura 78: Escolha do FQDN do AD DC

5. Na tela subsequente, *Domain NetBIOS Name*, escolha `DOMAINA` ou `DOMAINB` (dependendo do seu grupo) e clique em *Next*.

6. Na página *Set Forest Functional Level*, selecione o nível funcional de floresta que acomoda os controladores de domínio a serem instalados em qualquer lugar da floresta. Como teremos somente controladores de domínio Windows 2008 Server e acima, utilizaremos o nível funcional `Windows 2008 Server`. Confira sua seleção de acordo com a imagem a seguir, e clique em *Next*.

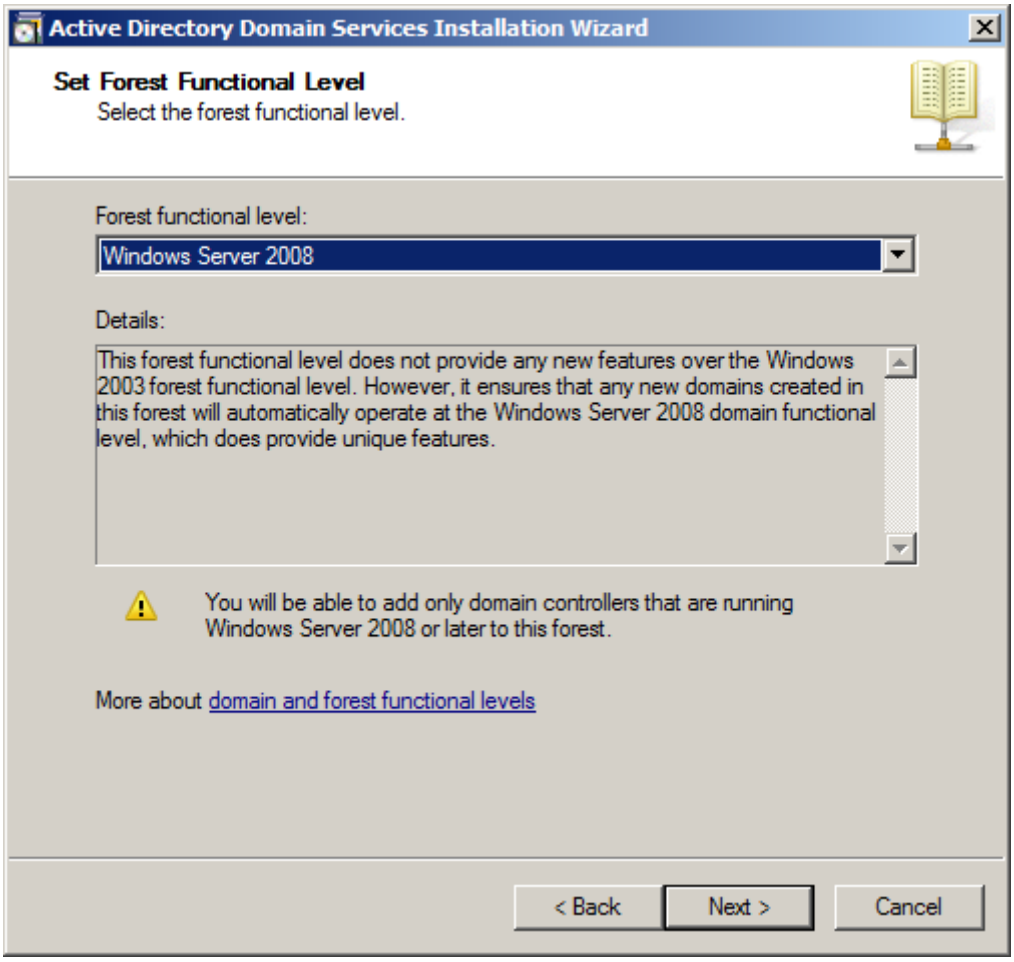

Figura 79: Escolha do nível funcional da floresta AD DC

7. Na tela *Additional Domain Controller Options*, mantenha a opção `DNS Server` marcada, indicando que a infraestrutura DNS da sua floresta deverá ser criada durante a instalação do AD DS. Em seguida, clique em *Next*.

   O sistema irá informar que uma delegação DNS para o servidor local (a máquina *WinServer-G*) não pode ser criada pois o servidor DNS autoritativo não está usando o servidor DNS do Windows, como se segue:

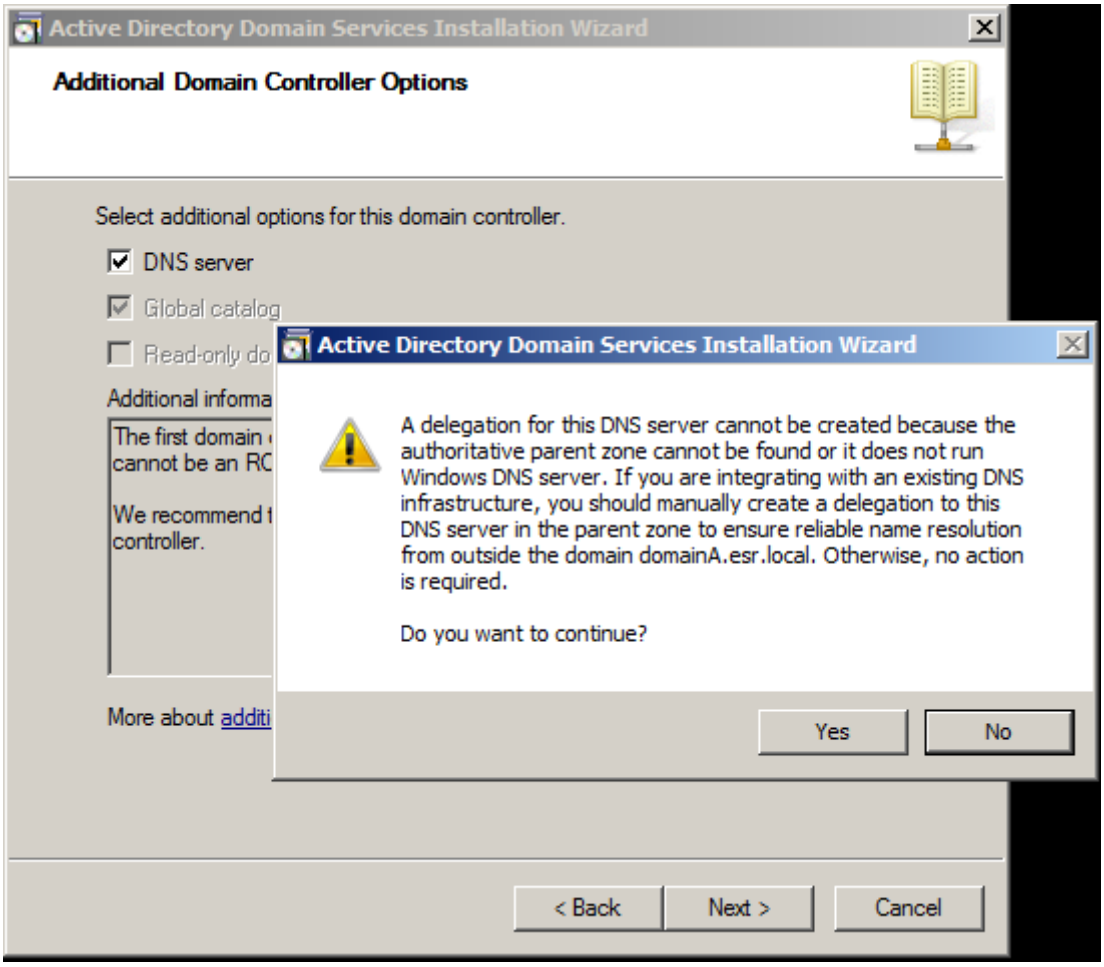

Figura 80: Erro na delegação DNS do AD DC

   Após ler a mensagem de aviso, clique em *Yes* para continuar.

8. Na tela *Location for Database, Log Files and SYSVOL*, mantenha os valores propostos pelo instalador e clique em *Next*.

9. Na tela *Directory Services Restore Mode Administrator Password*, defina uma senha para o modo de recuperação dos serviços de diretório do AD DC a ser usada em casos de falha. Para este exemplo, defina a senha como `rnpesr`, como mostrado abaixo. Em seguida, clique em *Next*.

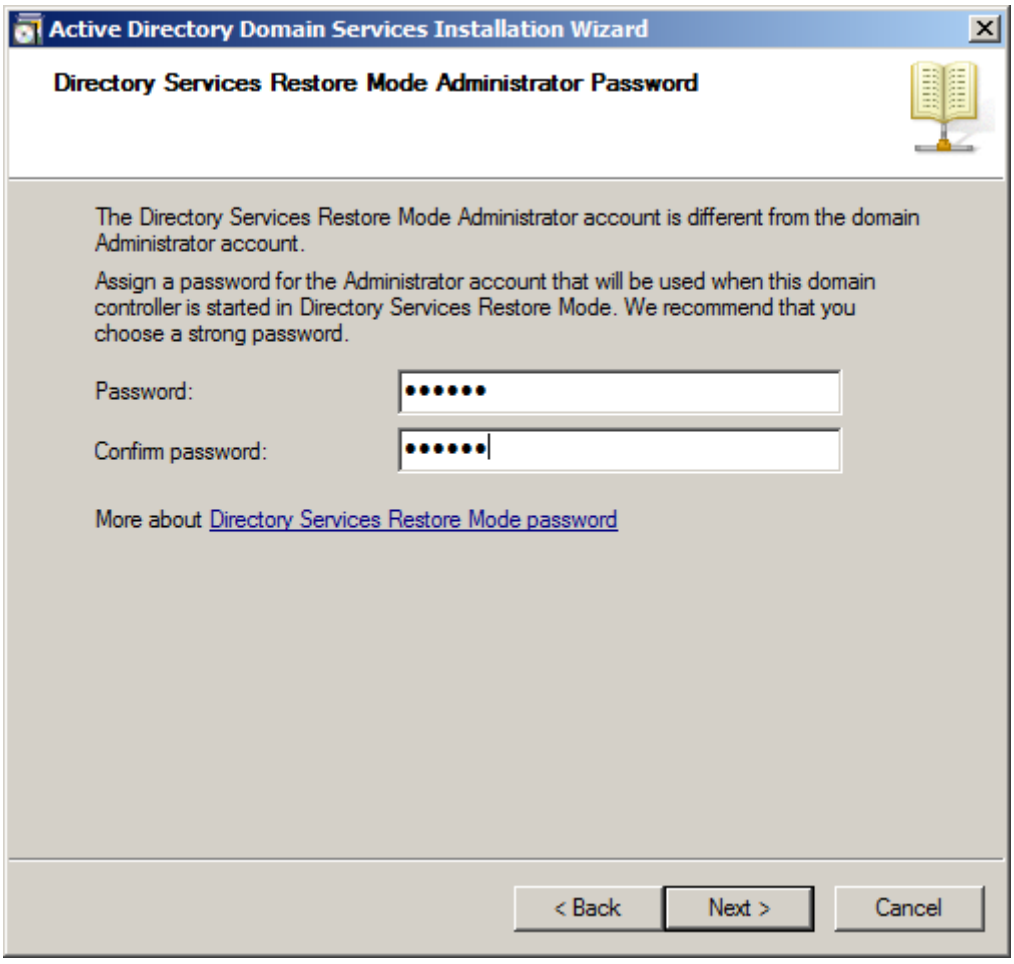

Figura 81: Definição da senha do modo de recuperação do AD DC

10. Na tela *Summary*, verifique se todas as opções definidas para o servidor do *Active Directory* estão corretas; em caso positivo, clique em *Next*.
11. Ao final do processo de instalação da *role* AD DC, reinicie a máquina *WinServer-G* para concluir o processo de instalação.

2) Configuração do firewall para o *Active Directory*

Esta atividade será realizada na máquina virtual *FWGW1-G*.

O próximo passo seria adicionar a máquina *WinClient-G* ao domínio mas, antes disso, temos que configurar a *chain* FORWARD do firewall *FWGW1-G* para permitir o repasse dos pacotes nas portas relevantes.

A base de documentação da Microsoft, acessível através do link (https://support.microsoft.com/en-us/help/832017#method1) lista um grande conjunto de portas a serem acessadas, como se segue:

- Para ambientes que utilizam exclusivamente versões do Windows anteriores ao Windows Server 2008 e Windows Vista, deve-se habilitar conectividade das portas 1025 a 5000.

- Para ambientes que utilizam apenas o Windows Server 2008 R2, Windows Server 2008, Windows 7 ou Windows Vista, deve-se habilitar conectividade das portas 49152 a 65535.
- Para ambientes que utilizam tanto versões modernas quanto antigas do Windows, deve-se habilitar ambas as faixas acima, 1025 a 5000 e 49152 a 65535.

Além dessas portas, a figura a seguir mostra também quais portas conhecidas devem ser liberadas pelo firewall para conectividade.

Application protocol	Protocol	Ports
Active Directory Web Services (ADWS)	TCP	9389
Active Directory Management Gateway Service	TCP	9389
Global Catalog	TCP	3269
Global Catalog	TCP	3268
ICMP		No port number
LDAP Server	TCP	389
LDAP Server	UDP	389
LDAP SSL	TCP	636
IPsec ISAKMP	UDP	500
NAT-T	UDP	4500
RPC	TCP	135
RPC randomly allocated high TCP ports[1]	TCP	1024 - 5000 49152 - 65535[2]
SMB	TCP	445

Figura 82: Portas conhecidas para liberação do AD no firewall

Considerando o grande número de portas em questão, iremos permitir a faixa completa de conexão entre as máquinas *WinServer-G* e *WinClient-G*, para facilitar a configuração neste laboratório.

1. Acesse a máquina *FWGW1-G* como usuário `root` e permita trânsito irrestrito de pacotes entre as máquinas *WinServer-G* e *WinClient-G*. Considere o sentido do fluxo de pacotes em suas regras.

```
# hostname ; whoami
FWGW1-A
root
```

```
# iptables -A FORWARD -s 10.1.1.10/32 -d 172.16.1.20/32 -j ACCEPT
```

3) Adição de clientes ao *Active Directory*

Esta atividade será realizada na máquina virtual *WinClient-G*.

1. Vamos, agora sim, adicionar a máquina *WinClient-G* ao domínio. Acesse-a como usuário `Aluno` e abra as configurações de rede. Acesse *Iniciar* e digite `ncpa.cpl`. Em seguida, clique com o botão direito em *Conexão Local* e navegue para *Propriedades* > *Protoloco TCP/IP Versão 4* > *Propriedades*. Altere o servidor DNS primário para o IP da máquina *WinServer-G*, como se segue:

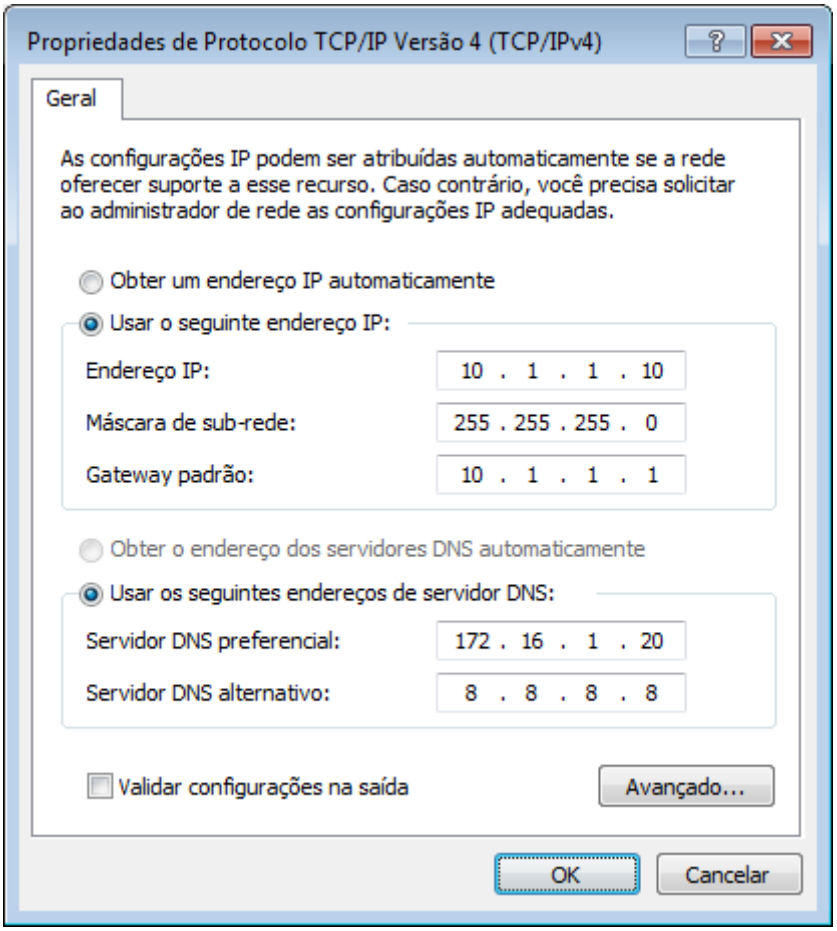

Figura 83: Configuração DNS do cliente AD

2. Agora, navegue para *Painel de Controle* > *Sistema e Segurança* > *Sistema* > *Alterar configurações*. Em seguida, clique no botão *Alterar...* para mudar o domínio da máquina local. Na caixa *Membro de*, marque o botão *Domínio* e digite o FQDN do domínio configurado no passo (4) da atividade (1) desta sessão, como se segue.

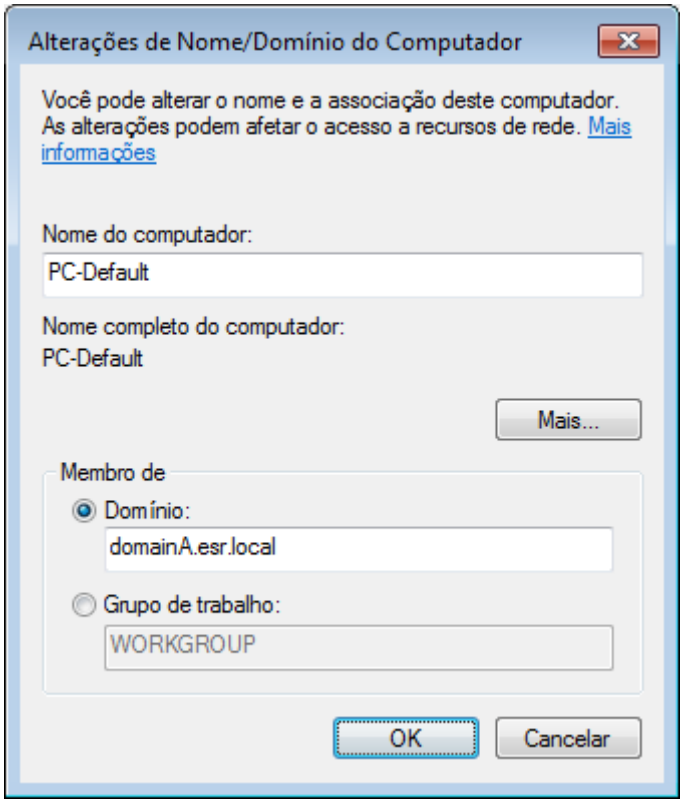

Figura 84: Inserindo o cliente AD no domínio

Clique em *OK*. O sistema irá exigir autenticação — você deve usar um usuário com permissões **administrativas** no AD DC, como o usuário `Administrator`. Informe, também, o domínio de autenticação do usuário. Trocando em miúdos, autentique-se como:

- Nome de usuário: `DOMAINA\Administrator`
- Senha: `rnpesr`

Após algum tempo de processamento, você deverá receber a mensagem *Bem vindo ao domínio domainG.esr.local*, como mostrado abaixo.

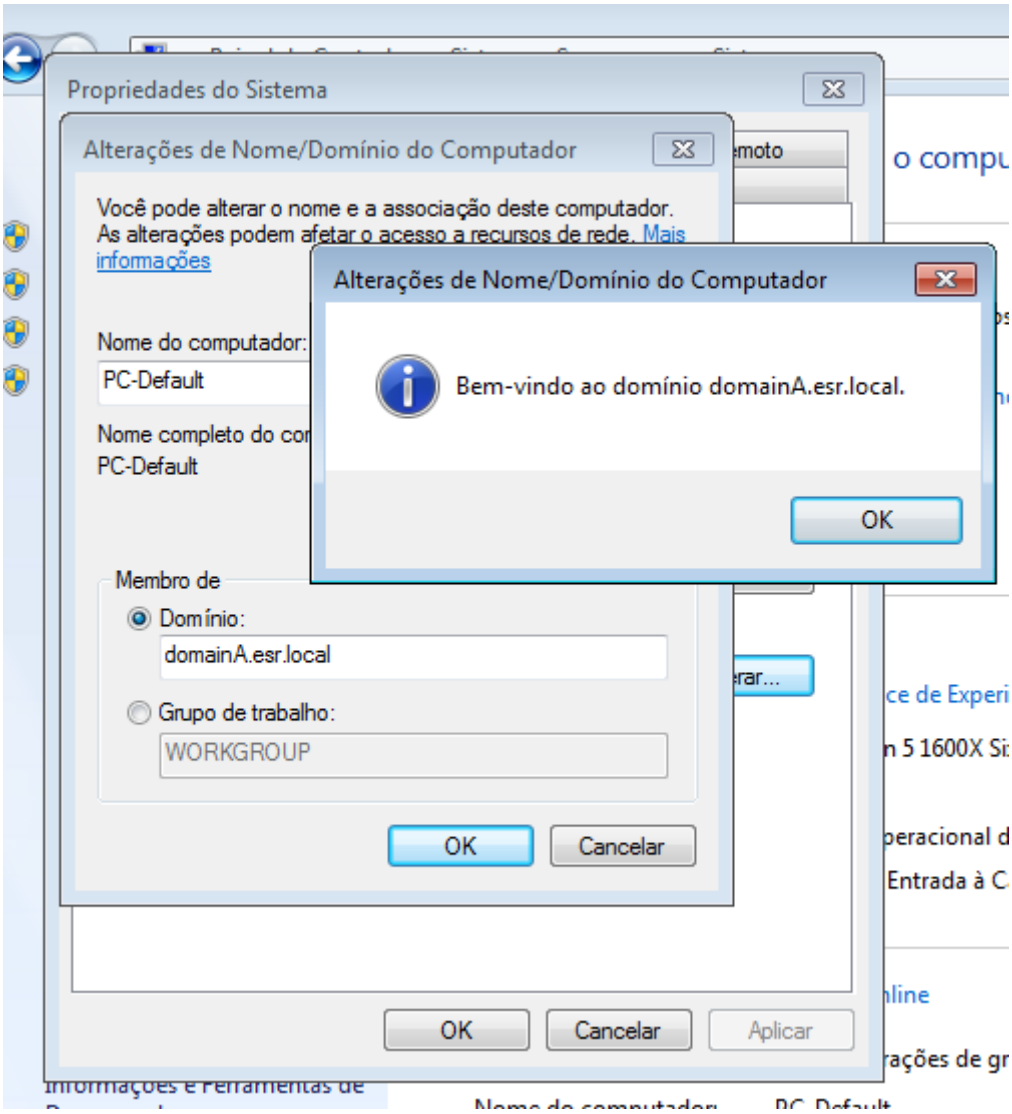

Figura 85: Inserção do cliente AD no domínio com sucesso

Reinicie a máquina *WinClient-G* para concluir o processo.

4) Adição de usuários ao *Active Directory*

Esta atividade será realizada nas máquinas virtuais *WinServer-G* e *WinClient-G*.

1. Vamos criar um usuário não-privilegiado para autenticar-se no domínio. Logue na máquina *WinServer-G* como um usuário administrativo (por exemplo, `DOMAINA\Administrator`), e execute *Start* > *Run...* > `dsa.msc`. Você deverá ver a tela do *Active Directory Users and Computers*, como se segue:

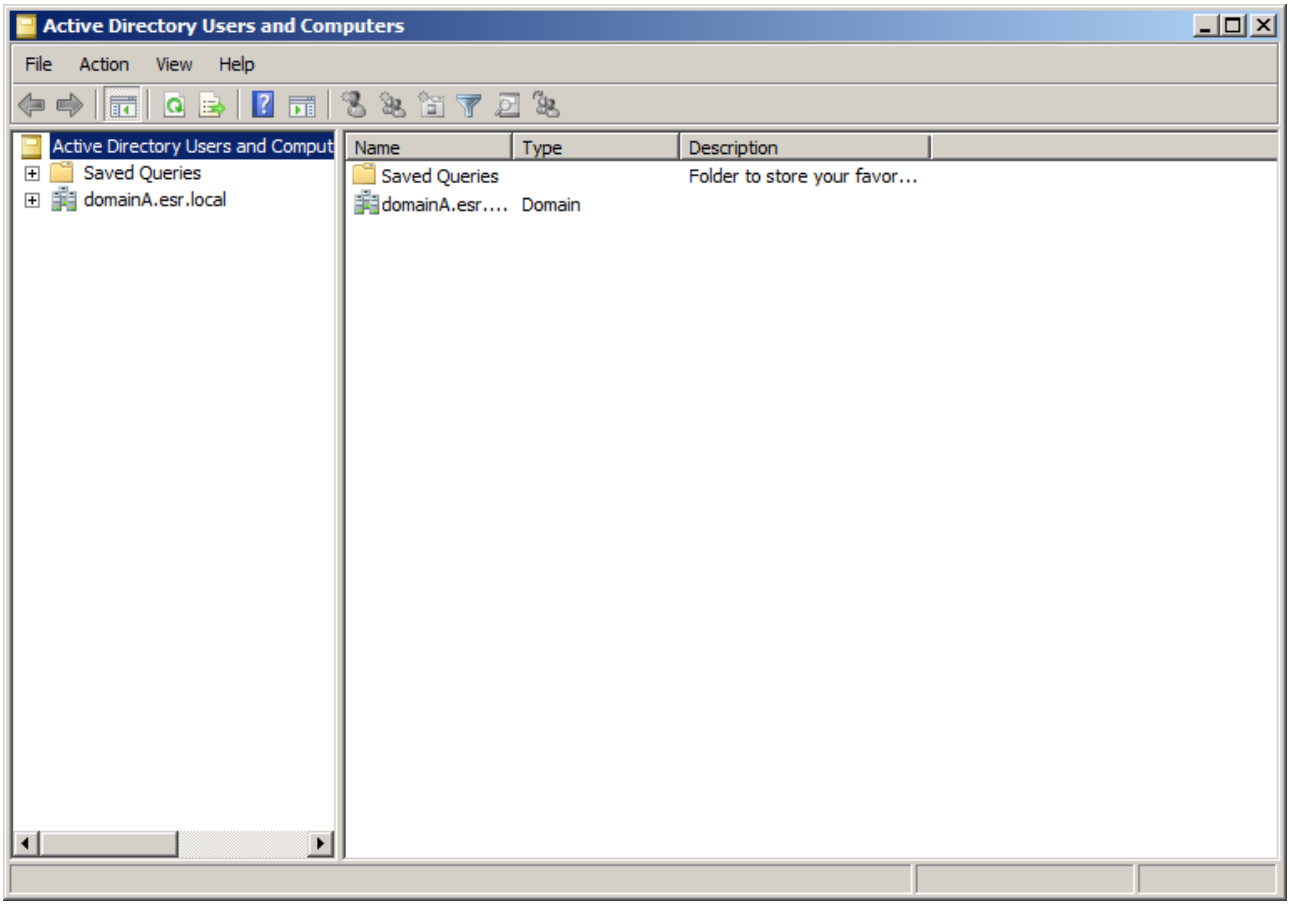

Figura 86: Interface de edição de usuários e máquinas do AD

2. Expanda a floresta `domainA.esr.local`, e observe as pastas *Builtin*, *Computers*, *Domain Controllers*, *ForeignSecurityPrincipals* e *Users*. Para visualizar os usuários e grupos existentes no domínio, clique sobre a pasta *Users*.

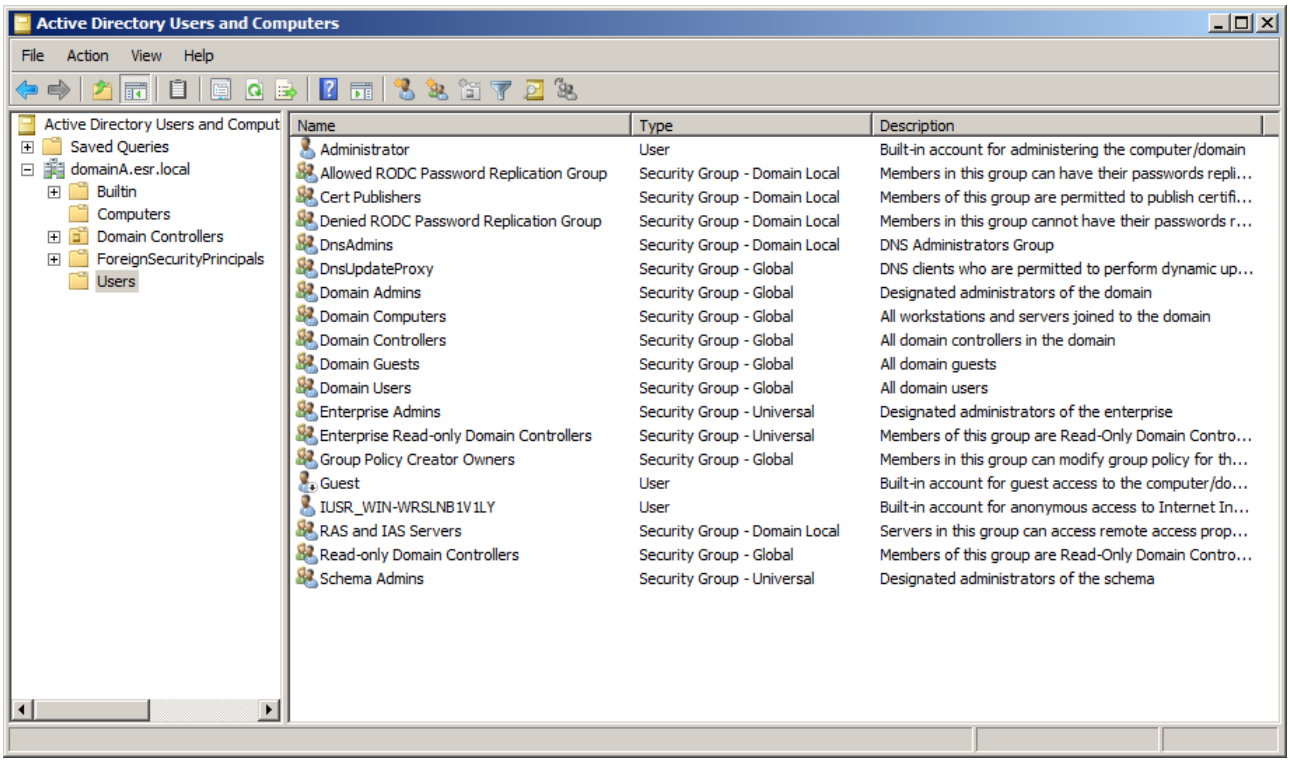

Figura 87: Visão de usuários e grupos existentes no AD

De igual forma, para ver os computadores adicionados ao AD, basta clicar sobre a pasta

Computers.

3. Para adicionar um novo usuário, clique com o botão direito sobre a pasta *Users*, e em seguida *New* > *User*. Crie um usuário com os seguintes dados:

   - *First name*: Indiana
   - *Last name*: Jones
   - *Initials*: IJ
   - *Full name*: Henry Walton Jones Jr.
   - *User logon name*: `indyjones@domainA.esr.local`
   - *User logon name (pre-Windows 2000)*: `DOMAINA\indyjones`

   Preenchidos os dados, clique em *Next*.

4. Na tela de definição de senha, devemos escolher uma senha suficientemente complexa para que o AD não a invalide. Uma senha como `RnpEsr!123` é uma boa escolha. Logo abaixo, mantenha marcada a caixa *User must change password at next logon*, e todas as demais desmarcadas. Clique em *Next*.
5. Na tela de confirmação dos dados, verifique que tudo está correto como mostrado a seguir, e clique em *Finish*.

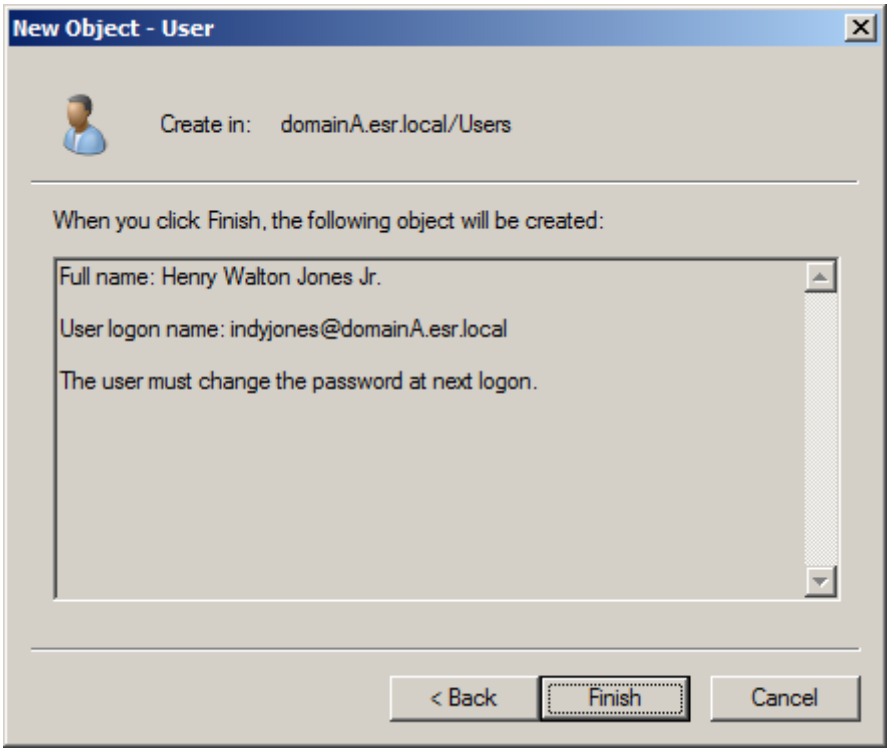

Figura 88: Confirmação de adição de usuário ao AD

6. De volta à máquina *WinClient-G*, tente logar com o usuário `indyjones` recém-criado. Clique no botão *Trocar Usuário* > *Outro Usuário* e digite os dados inseridos nos passos (3) e (4). Observe que o logon será feito no domínio `DOMAINA`, como objetivado.

Figura 89: Logon inicial no AD

Imediatamente, o AD reporta que a senha deve ser alterada no primeiro logon — isso faz sentido, pois mantivemos a caixa *User must change password at next logon* marcada quando da criação do usuário no passo (4). Escolha uma nova senha, diferente da primeira e igualmente complexa (sugestão: `Seg2@rnp!`), e confirme o logon.

Finalmente, verifique que você está de fato logado na máquina como o usuário do domínio.

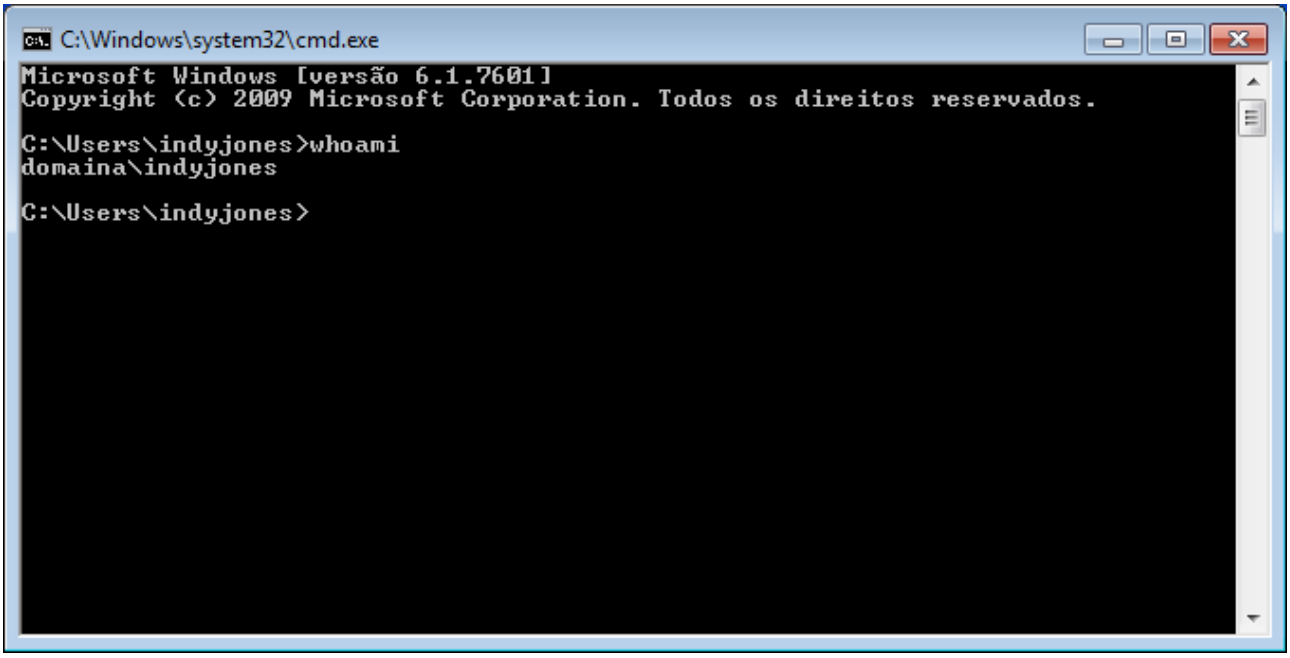

Figura 90: Verificação de logon no AD

5) Distribuição de configurações via GPOs

Esta atividade será realizada nas máquinas virtuais *FWGW1-G*, *WinServer-G* e *WinClient-G*.

Iremos agora usar GPOs (*Group Policy Objects*) para fazer configurações centralizadas de máquinas clientes do domínio. De fato, iremos usar as GPOs para resolver um problema que já tivemos anteriormente neste curso: a adição de certificados de ACs para *man-in-the-middle*, especificamente o do Squid *SslBump Peek and Splice* (sessão 7, atividade 2).

1. Primeiro, acesse a máquina *FWGW1-G* como usuário `root` e volte a executar o Squid em modo de interceptação de tráfego SSL, como fizemos anteriormente. Caso as regras de firewall não estejam mais ativas, reinsira-as e execute o Squid:

```
# hostname ; whoami
FWGW1-A
root
```

```
# iptables -t nat -A PREROUTING -i eth2 -p tcp -m tcp --dport 80 -j REDIRECT --to
-port 8080
# iptables -t nat -A PREROUTING -i eth2 -p tcp -m tcp --dport 443 -j REDIRECT --to
-port 8443
# iptables -A INPUT -s 10.1.1.0/24 -p tcp -m tcp -m multiport --dports 8080,8443 -j
ACCEPT
```

```
# /usr/local/sbin/squid -f /usr/local/etc/squid.conf
```

2. Na máquina *WinClient-G*, tente acessar um website via HTTPS para testar se a interceptação está ativa. No exemplo abaixo, estamos acessando o https://facebook.com ; note que o certificado é identificado como inválido (como esperado), e emitido pela CA da máquina `fwgw1-g.esr.rnp.br`:

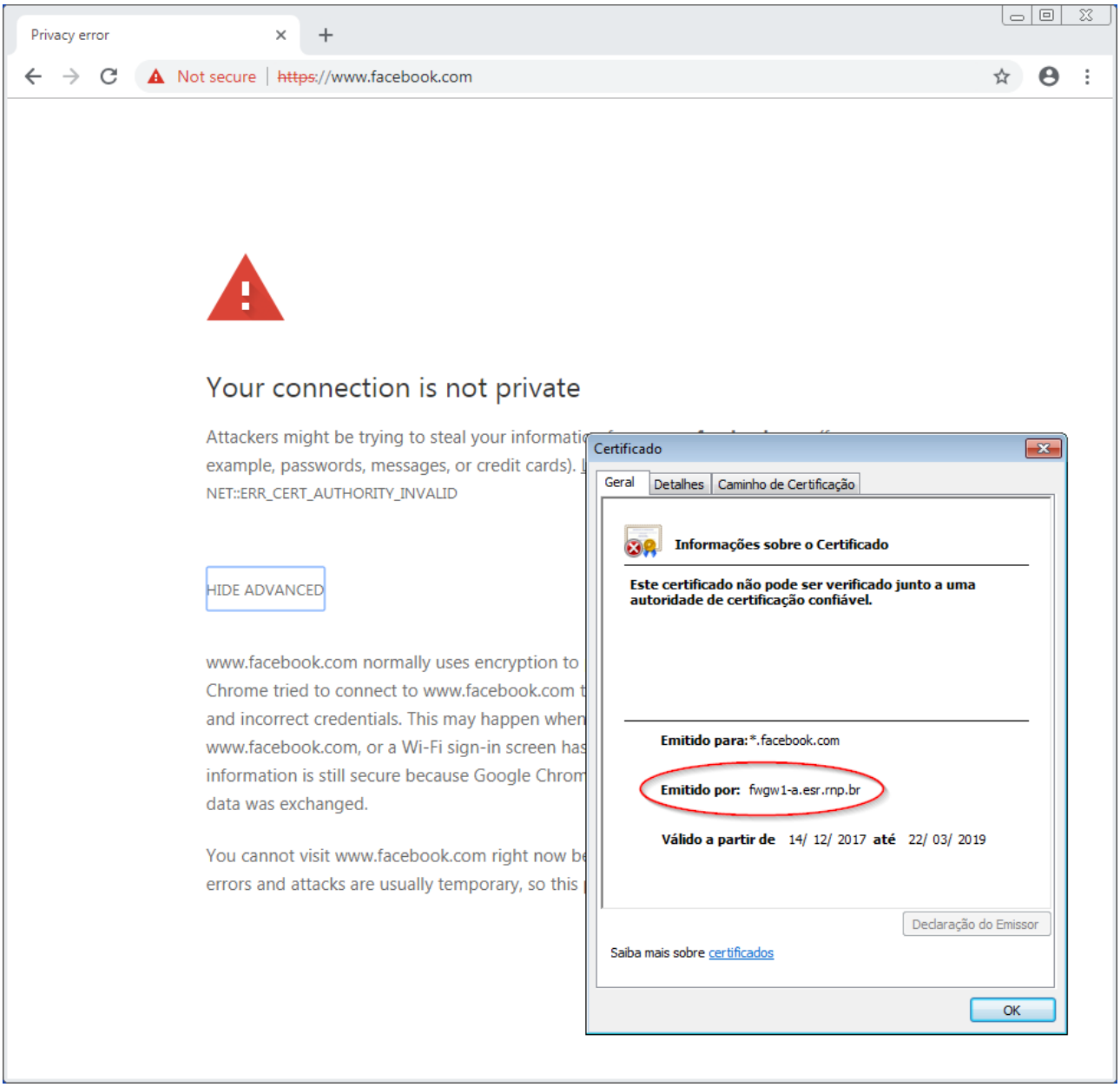

Figura 91: Detecção de certificado forjado não-confiável na máquina WinClient-G

3. Para resolver o problema, vamos adicionar o certificado do Squid instalado na máquina *FWGW1-G* à base de certificados raiz confiáveis, como fizemos anteriormente. Mas, ao invés de fazer isso manualmente, vamos usar o AD e as GPOs para realizar essa tarefa. Copie o certificado localizado em `/usr/local/etc/ssl/public.crt` (na máquina *FWGW1-G*) para o *Desktop* da máquina *WinServer-G* — use o programa `WinSCP` ou a pasta compartilhada pelo Virtualbox, como preferir.

   Ao final do processo, você deverá ter a chave pública da CA do Squid disponível na máquina *WinServer-G*, como mostrado abaixo.

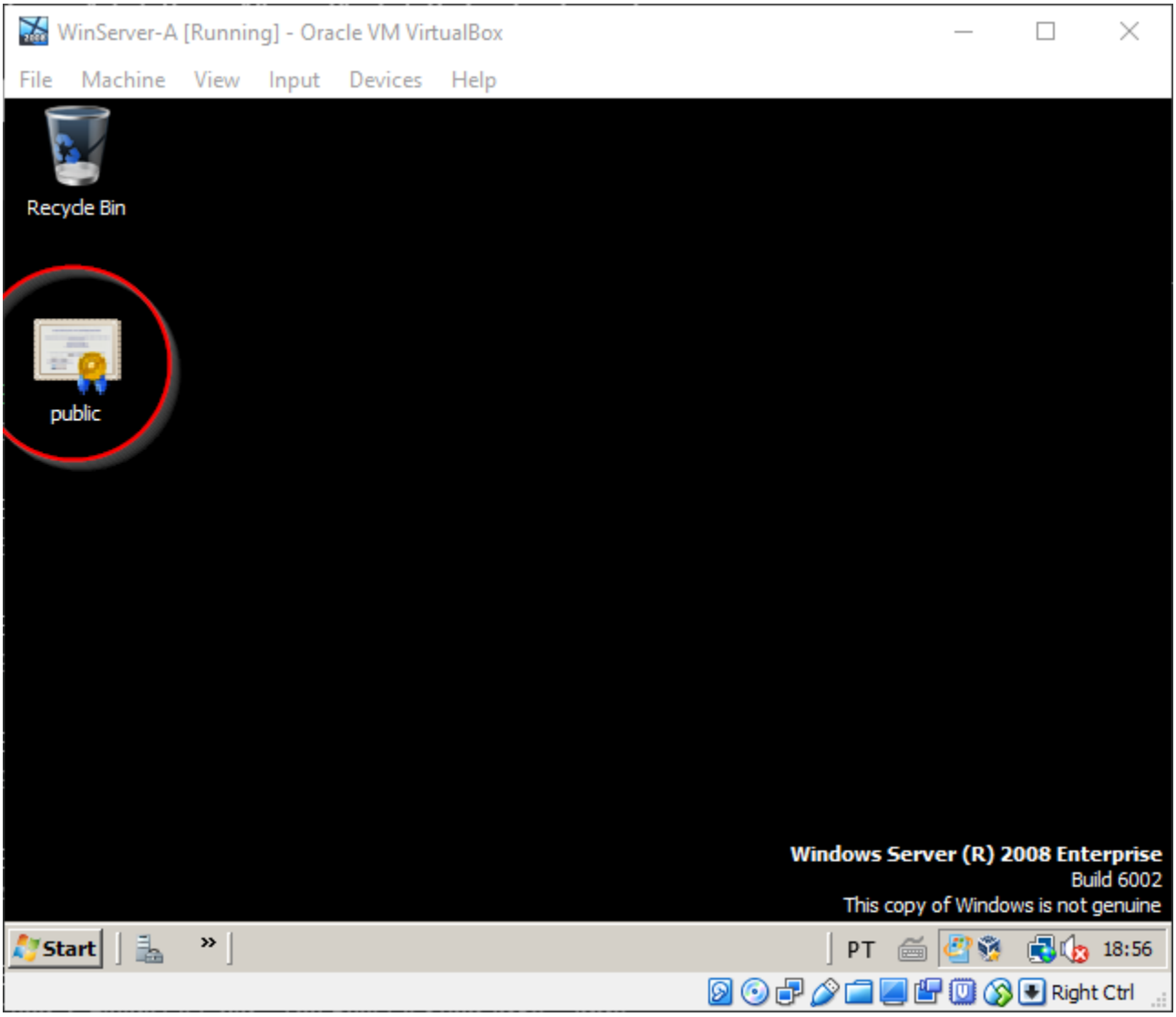

Figura 92: Cópia do certificado da CA do Squid para a máquina WinServer-G

4. Vamos criar uma política para distribuição do certificado copiado. Execute *Start* > *Run...* > `gpmc.msc`. Você deverá ver a tela do *Group Policy Management*, como se segue:

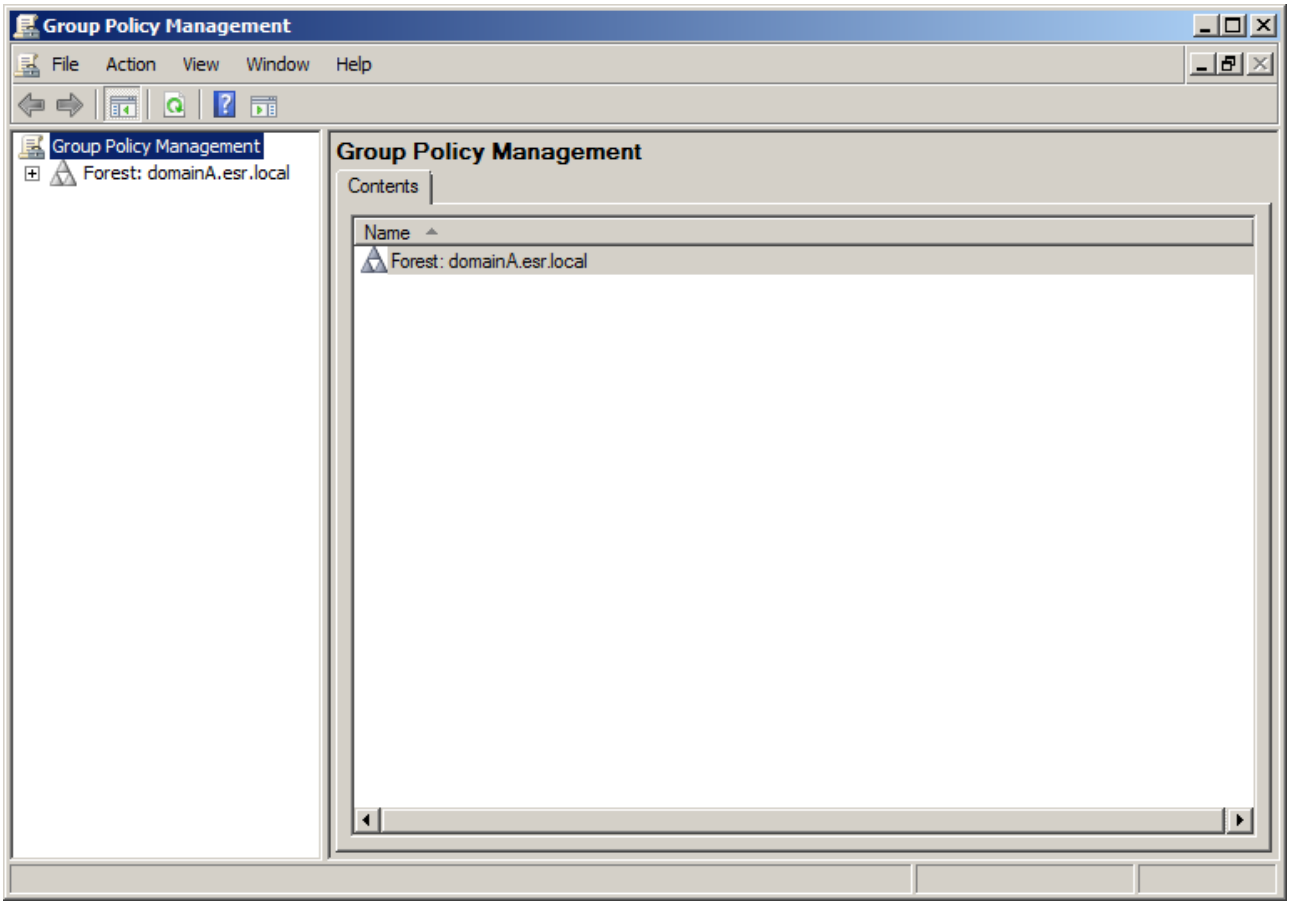

Figura 93: Ferramenta para gestão de políticas no AD

5. Expanda a floresta `domainA.esr.local`, e em seguida *Domains*. Clique com o botão direito no domínio `domainA.esr.local`, e em seguida em *Create a GPO in this domain, and Link it here...*. Para o nome da GPO, digite *squidcert*, e em seguida clique em *OK*. Uma nova política deve surgir na lista linkadas, como mostrado abaixo:

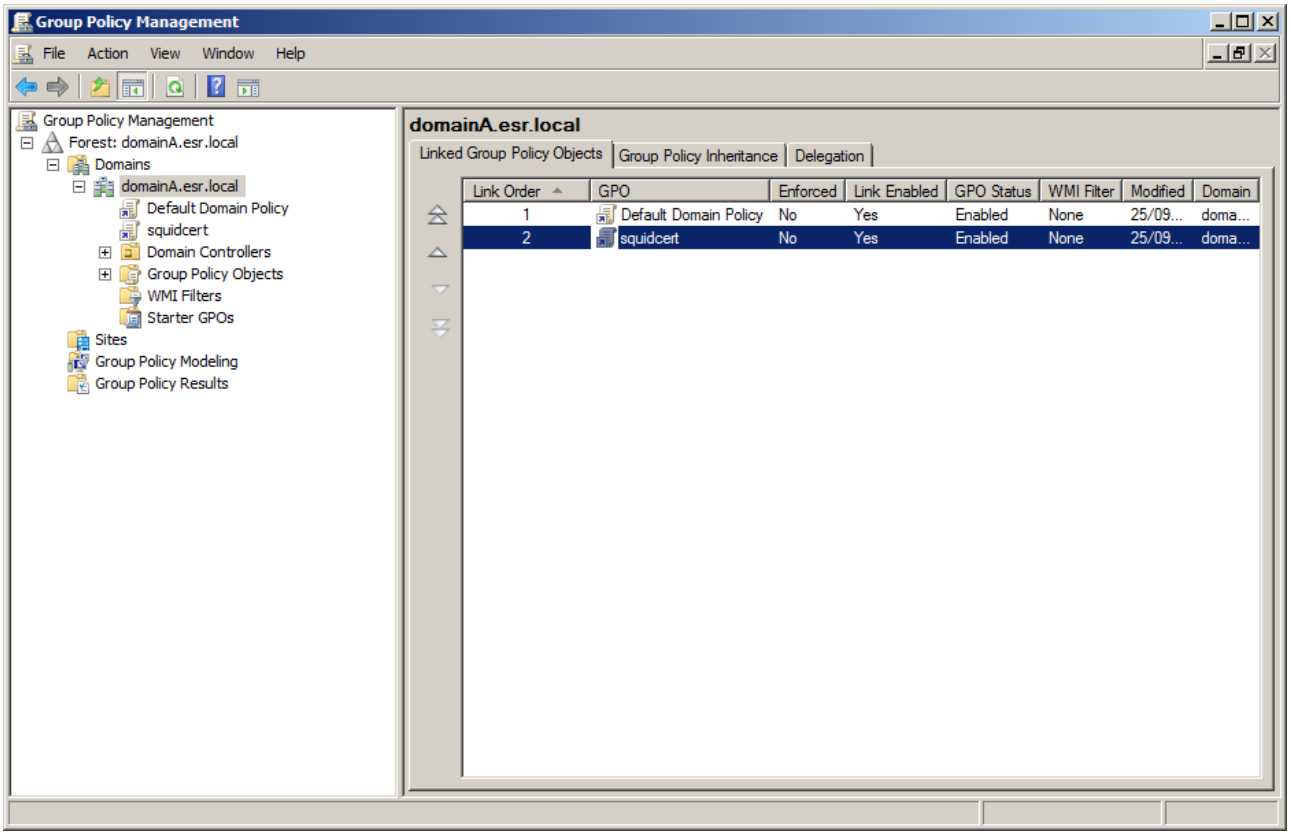

Figura 94: Criação de nova GPO

6. Clique com o botão direito na política *squidcert*, e em seguida em *Edit*. Surgirá uma nova janela para edição de políticas, idêntica à invocada pelo *snap-in* `gpedit.msc`. Navegue para *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Public Key Policies*, clique com o botão direito em *Trusted Root Certification Authorities*, como mostrado abaixo. Em seguida, clique em *Import*.

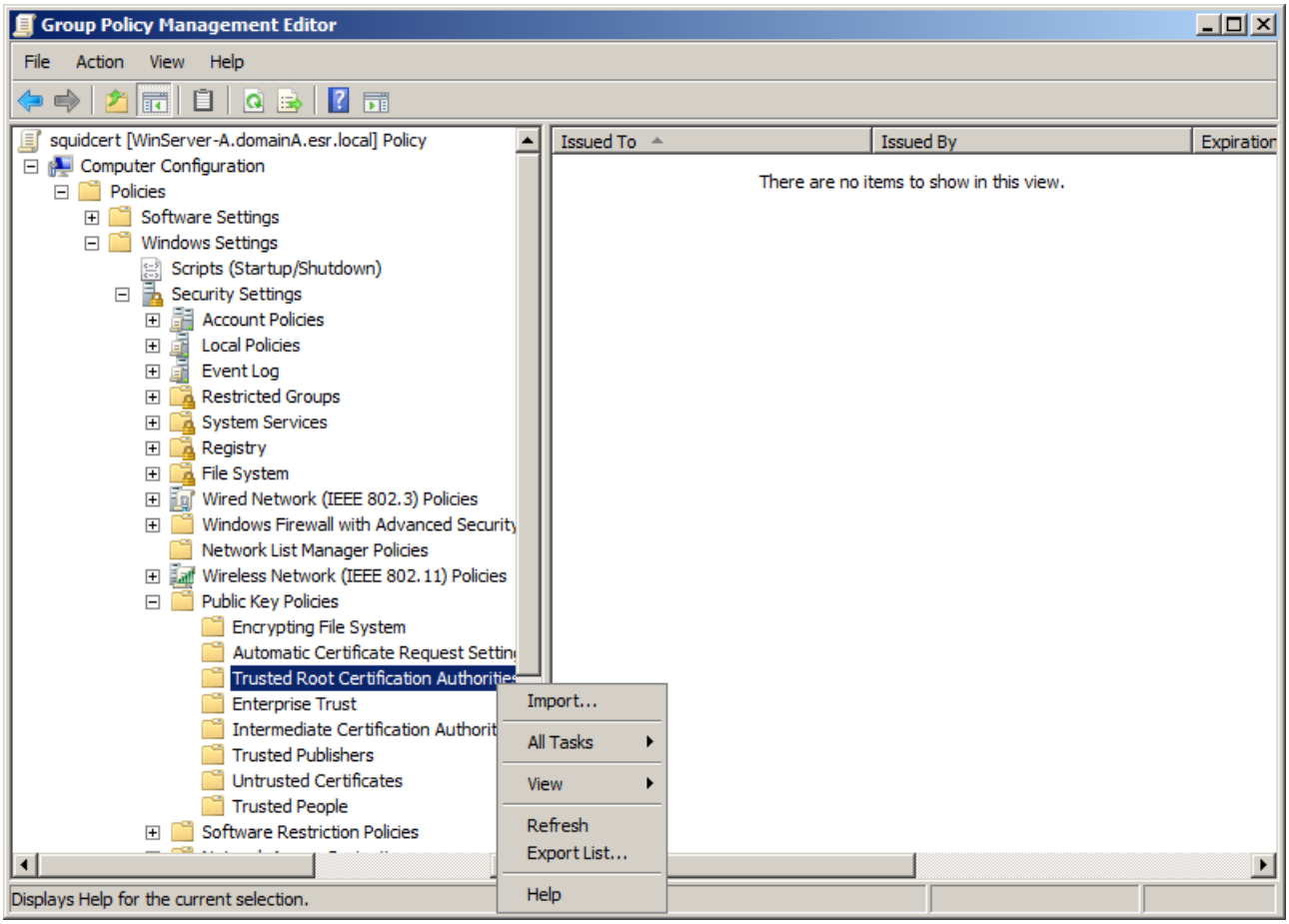

Figura 95: Navegando na tela de edição de políticas

7. Será aberta uma tela de adição de certificado idêntica à que usamos na sessão 7. Aponte o certificado do Squid baixado no passo (3) desta atividade, e confirme todas as janelas de adição do certificado. Ao final, você deverá vê-lo adicionado ao *Trusted Root Certification Authorities* da GPO, como mostrado a seguir.

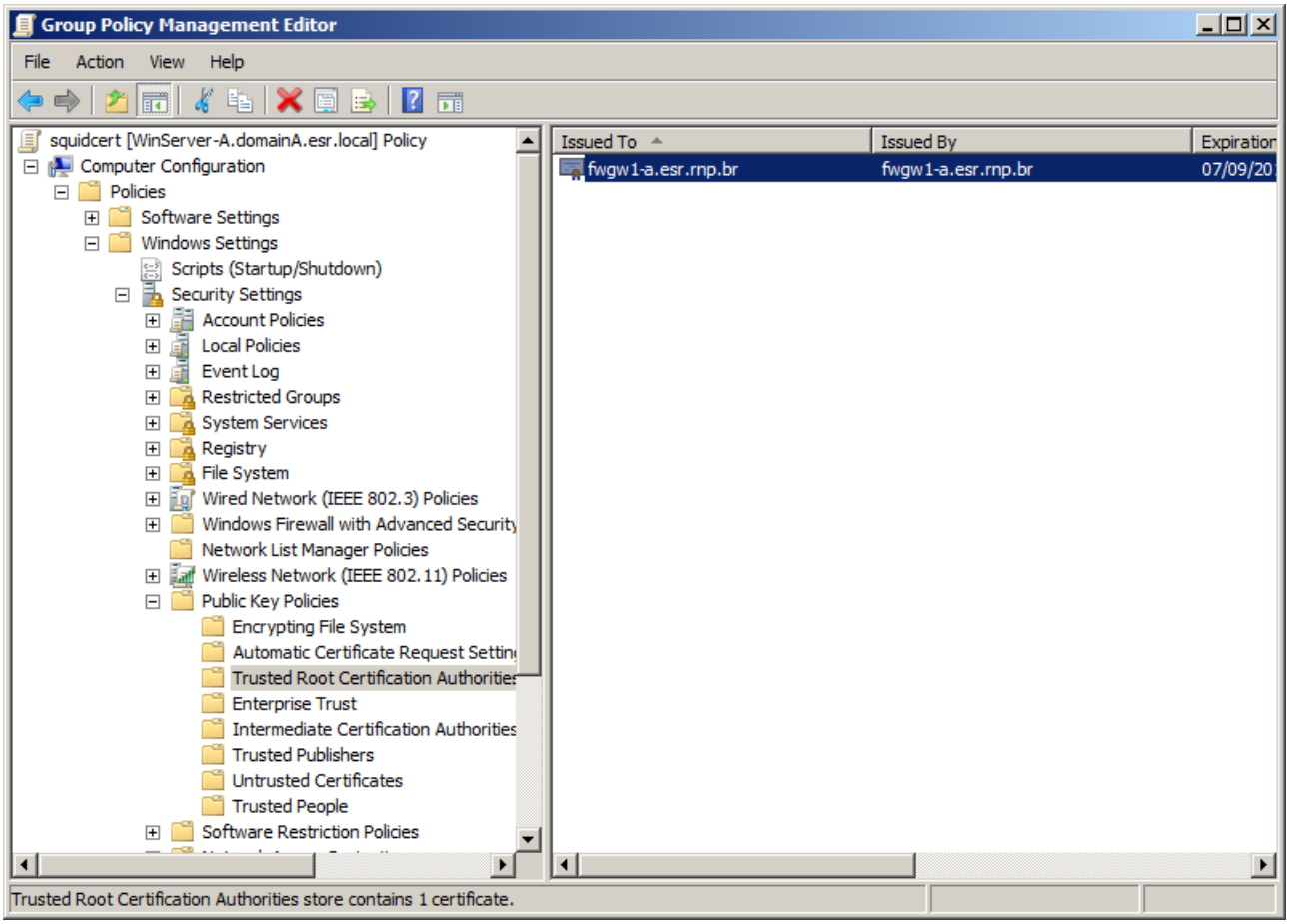

Figura 96: Certificado do Squid adicionado à GPO

8. Tudo pronto! Feche a janela do *Group Policy Management Editor* e do *Group Policy Management*, e volte à máquina *WinClient-G*. Segundo a *knowledge base* da Microsoft (https://msdn.microsoft.com/en-us/library/ms813077.aspx), as GPOs são atualizadas de 90 em 90 minutos, com *offsets* aleatórios de 30 minutos. Como não queremos esperar tudo isso para verificar nossa configuração, abra (novamente, na máquina *WinClient-G*) uma janela do *prompt* de comando e digite `gpupdate /force` para atualizar as GPOs imediatamente:

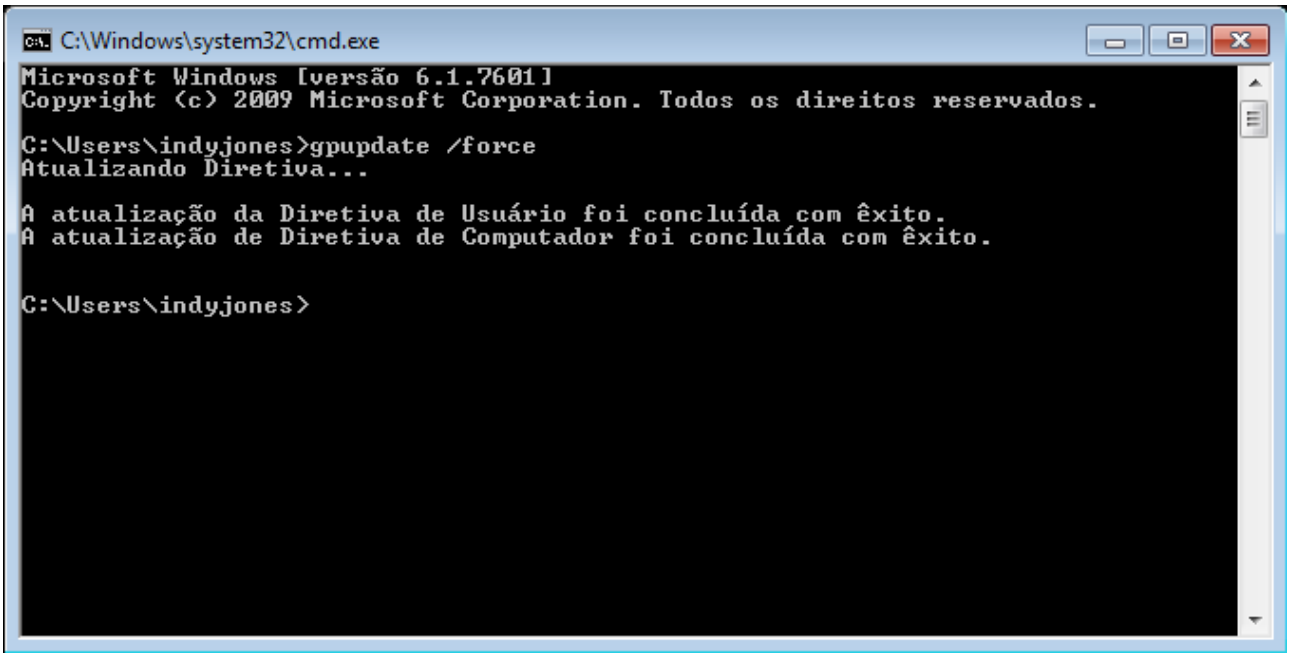

Figura 97: Forçando atualização de GPOs imediatamente

9. Abra o navegador e tente acessar um website em HTTPS, como o https://facebook.com que havia sido acessado anteriormente. Note que, agora, o navegador reporta o certificado forjado pela CA do Squid como confiável.

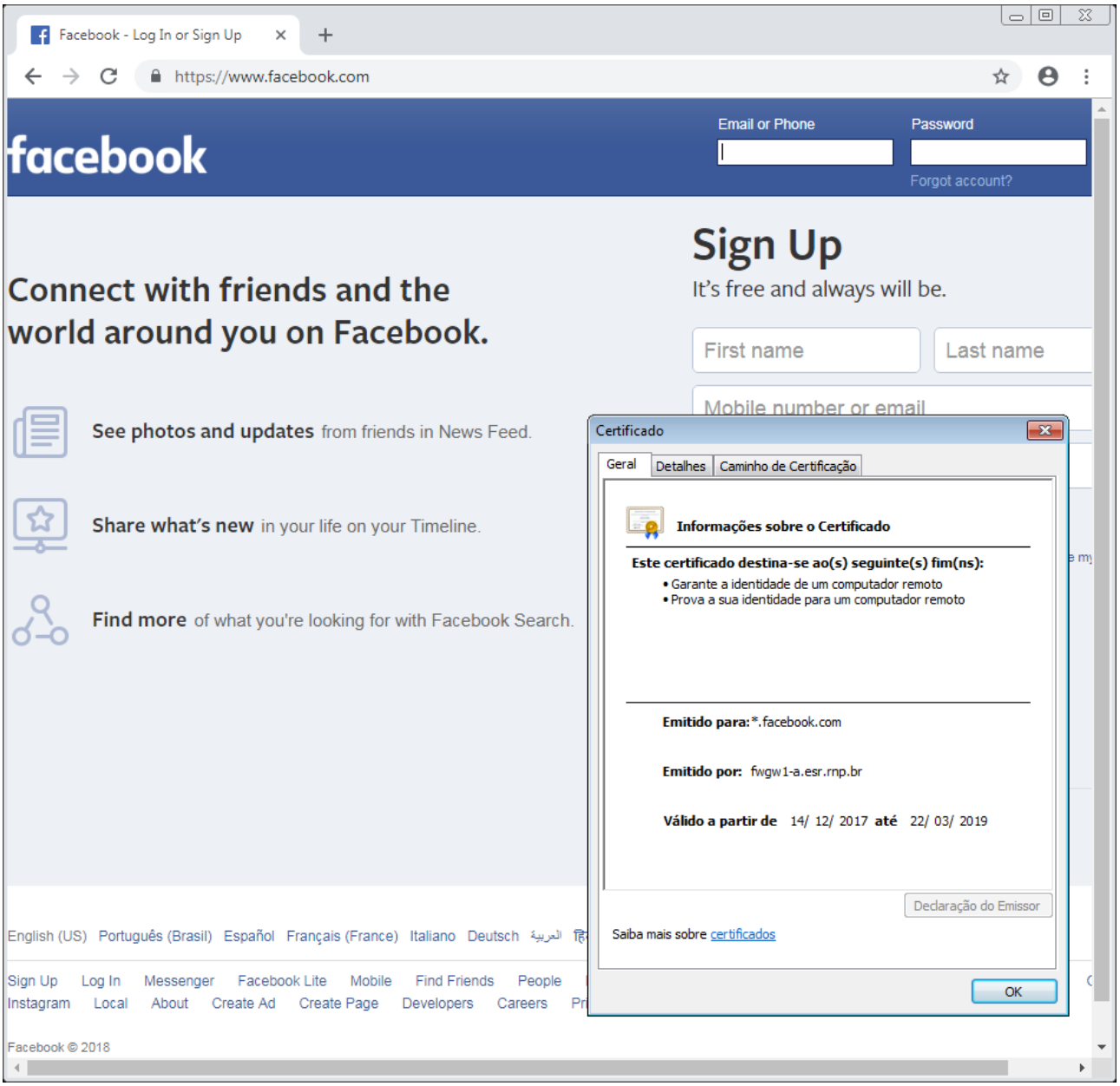

Figura 98: Detecção de certificado da CA do Squid como confiável

10. De fato, verificando a lista de certificados raiz confiáveis do sistema, o da máquina *FWGW1-G* consta da lista.

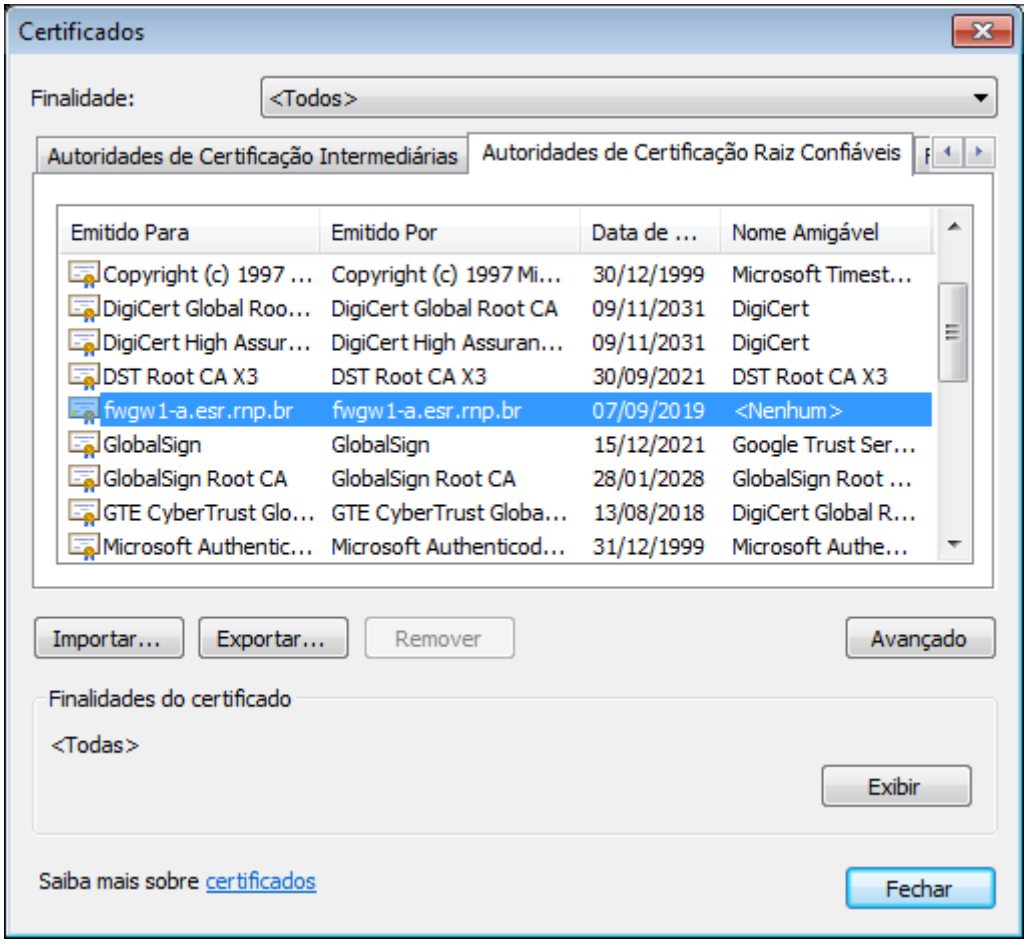

Figura 99: Certificado da CA do Squid adicionado à lista de certificadoras raiz confiáveis

Com efeito, nossa configuração via GPO funcionou corretamente — em um cenário com dezenas de clientes Windows, ou mesmo centenas, você poderia usar um esquema de configuração como este para distribuir o certificado do seu *proxy* de forma imediata.

6) Configuração do WSUS

Esta atividade será realizada nas máquinas virtuais *WinServer-G* e *WinClient-G*.

1. Acesse a máquina *WinServer-G* como um usuário administrativo (por exemplo, `DOMAINA\Administrator`) e verifique que todos as atualizações de segurança da Microsoft estão aplicadas. Execute *Start* > *Windows Update* e verifique que o servidor está totalmente atualizado, como mostrado abaixo.

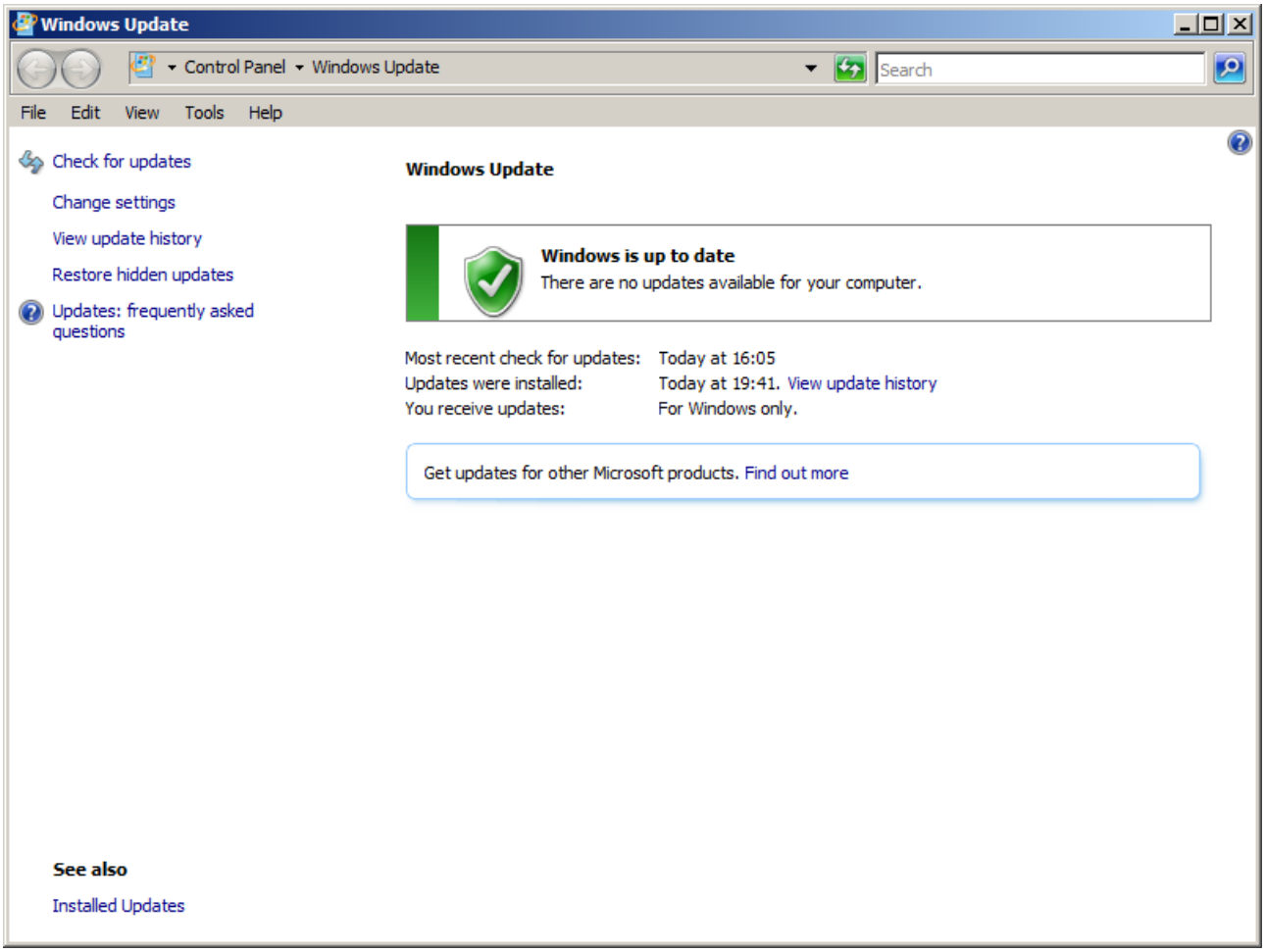

Figura 100: Máquina WinServer-G atualizada

2. Ainda na máquina *WinServer-G*, abra o *Server Manager* e em seguida navegue para *Roles* > *Add Roles*. Na nova janela, marque a caixa do *Windows Server Update Services* (WSUS), aceite a adição dos *role services* requeridos como dependência para ele, e confirme todos os valores padrão para instalação da *role*.