FORMAÇÃO EM SEGURANÇA CIBERNÉTICA

CADERNO DE ATIVIDADES

Segunda Semana

Rua Lauro Müller, 116 sala 1103

22290-906 Rio de Janeiro, RJ

Diretor Geral

Nelson Simões

Diretor de Serviços e Soluções

José Luiz Ribeiro Filho

Escola Superior de Redes

Coordenação

Luiz Coelho

Equipe ESR (em ordem alfabética)

Celia Maciel, Cristiane Oliveira, Derlinéa Miranda, Edson Kowask, Elimária Barbosa, Evellyn Feitosa, Felipe Nascimento, Lourdes Soncin, Luciana Batista, Renato Duarte, Sérgio Souza e Yve Abel Marcial.

Versão 0.1.1

Índice

Sessão 1: Configuração preliminar das máquinas

1) Da divisão de grupos

Neste curso, os alunos serão divididos em dois grupos: `A` e `B`. Ao longo da semana, iremos realizar algumas atividades que vão envolver a intercomunicação entre máquinas virtuais dos alunos de cada grupo; para que as configurações de rede de dois alunos envolvidos em uma mesma atividade não conflitem, iremos adotar uma nomenclatura de endereços para cada grupo, como se segue:

Tabela 1. Nomenclatura entre grupos

Grupo	Sufixo de endereço
A	1
B	2

O que isso significa, na prática? Em vários momentos, ao ler este material, você irá se deparar com endereços como 172.16.G.20 ou 10.1.G.10 — que evidentemente são inválidos. Nesse momento, substitua o número do seu grupo pela letra `G` no endereço. Se você for membro do grupo `B`, portanto, os endereços acima seriam 172.16.2.20 e 172.16.2.10.

2) Topologia geral de rede

A figura abaixo mostra a topologia de rede que será utilizada durante este curso. Nos tópicos que se seguem, iremos verificar que a importação de máquinas virtuais, configurações de rede e conectividade estão funcionais antes de prosseguir. As configurações específicas de cada máquina/interface serão detalhadas na seção a seguir.

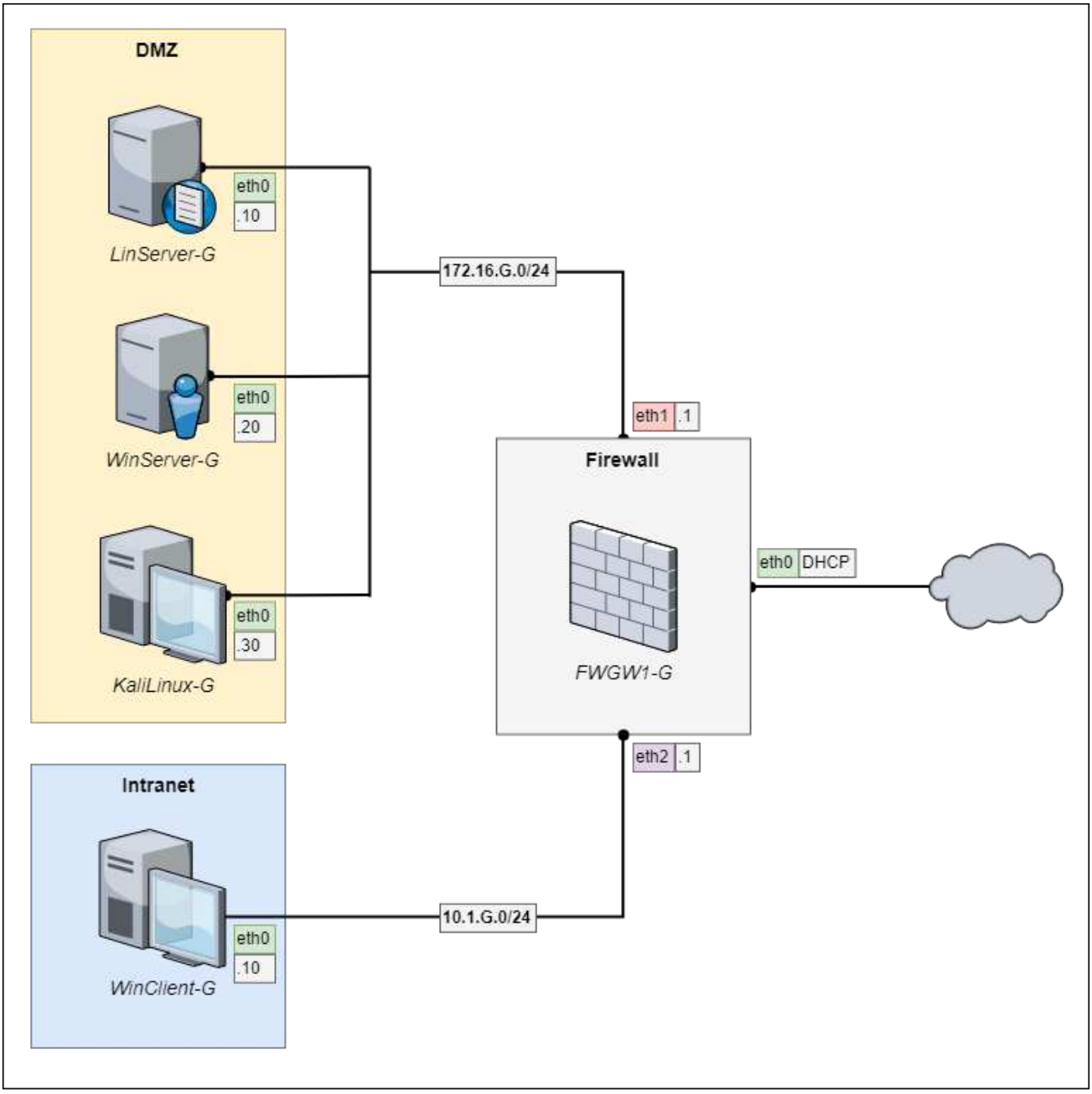

Figura 1: Topologia de rede do curso

3) Configuração do Virtualbox

1. Primeiramente, verifique se todas as máquinas virtuais foram importadas.

   Se ainda não foram, importe-as manualmente através do menu *File* > *Import Appliance*. Navegue até a pasta onde se encontra o arquivo `.ova` com as imagens das máquinas virtuais e clique em *Next*. Na tela subsequente, marque a caixa *Reinitialize the MAC address of all network cards* e só depois clique em *Import*.

   Ao final do processo, você deve ter cinco VMs com as configurações que se seguem.

   Tabela 2. VMs disponíveis no Virtualbox

Nome VM	**Memória**
FWGW1-G	2048 MB
LinServer-G	2048 MB
WinServer-G	2048 MB
KaliLinux-G	2048 MB
WinClient-G	2048 MB

   Se a quantidade de RAM de alguma das máquinas for inferior aos valores estipulados, ajuste-a.

2. Agora, configure as redes do Virtualbox. Acesso o menu *File* > *Host Network Manager* e crie as seguintes redes:

   Tabela 3. Redes host-only no Virtualbox

Rede	**Endereço IPv4**	**Máscara de rede**	**Servidor DHCP**
Virtualbox Host-Only Ethernet Adapter	172.16.G.254	255.255.255.0	Desabilitado
Virtualbox Host-Only Ethernet Adapter #2	10.1.G.254	255.255.255.0	Desabilitado

3. Finalmente, configure as interfaces de rede de cada máquinas virtual. Para cada VM, acesse *Settings* > *Network* e faça as configurações que se seguem:

Tabela 4. Interfaces de rede das máquinas virtuais

VM Nome	Interface	Conectado a	Nome da rede
FWGW1-G	Adapter 1	Bridged Adapter	Placa de rede física do *host*
	Adapter 2	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
	Adapter 3	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter #2
LinServer-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
WinServer-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
KaliLinux-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
WinClient-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter #2

4) Detalhamento das configurações de rede

As configurações de rede realizadas internamente em cada máquina virtual foram apresentados de forma sucinta na figura 1. Iremos detalhar as configurações logo abaixo:

Tabela 5. Configurações de rede de cada VM

VM Nome	Interface	Modo	Endereço	Gateway	Servidores DNS
FWGW1-G	eth0	Estático	DHCP	Automático	Automático
	eth1	Estático	172.16.G.1/24	n/a	n/a
	eth2	Estático	10.1.G.1/24	n/a	n/a
LinServer-G	eth0	Estático	172.16.G.10/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
WinServer-G	eth0	Estático	172.16.G.20/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
KaliLinux-G	eth0	Estático	172.16.G.30/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
WinClient-G	eth0	Estático	10.1.G.10/24	10.1.G.1	8.8.8.8 ; 8.8.4.4

5) Configuração da máquinas virtuais

Agora, vamos configurar a rede de cada máquina virtual de acordo com as especificações da topologia de rede apresentada no começo deste capítulo.

Observe que as máquinas virtuais da **DMZ** e **Intranet** ainda não terão acesso à Internet neste passo, pois ainda não configuramos o firewall. A próxima seção irá tratar deste tópico.

Para tangibilizar os exemplos nas configurações-modelo deste gabarito, iremos assumir que o aluno é membro do grupo `A`, ou seja, tem suas máquinas virtuais nas redes 172.16.1.0/24 e 10.1.1.0/24. Se você for membro do grupo `B`, tenha o cuidado de sempre adaptar os endereços IP dos exemplos para as suas faixas de rede.

1. Primeiramente, ligue a máquina *FWGW1-G* e faça login como usuário `root` e senha `rnpesr`. Verifique se o mapa de teclado está correto (teste com os caracteres `/` ou `ç`). Se não estiver, execute o comando:

   ```
   # dpkg-reconfigure keyboard-configuration
   ```

   Nas perguntas que se seguem, responda:

   Tabela 6. Configurações de teclado

Pergunta	**Parâmetro**
Keyboard model	Generic 105-key (Intl) PC
Keyboard layout	Other > Portuguese (Brazil) > Portuguese (Brazil)
Key to function as AltGr	Right Alt (AltGr)
Compose key	Right Logo key

   Finalmente, execute o comando que se segue. Volte a testar o teclado e verifique seu funcionamento.

   ```
   # systemctl restart keyboard-setup.service
   ```

2. Ainda na máquina *FWGW1-G*, edite o arquivo `/etc/network/interfaces` como se segue, reinicie a rede e verifique o funcionamento:

```
# hostname
FWGW1-A

# whoami
root

# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto eth0 eth1 eth2

iface eth0 inet dhcp

iface eth1 inet static
address 172.16.1.1
netmask 255.255.255.0

iface eth2 inet static
address 10.1.1.1
netmask 255.255.255.0

# systemctl restart networking

# ip a s | grep '^ *inet '
    inet 127.0.0.1/8 scope host lo
    inet 192.168.1.203/24 brd 192.168.1.255 scope global eth0
    inet 172.16.1.1/24 brd 172.16.1.255 scope global eth1
    inet 10.1.1.1/24 brd 10.1.1.255 scope global eth2
```

3. Ligue a máquina *LinServer-G* e faça login como usuário `root` e senha `rnpesr`. Se encontrar problemas com o teclado, aplique a mesma solução utilizada na etapa (1) desta atividade. A seguir, edite as configurações de rede no arquivo `/etc/network/interfaces`, de DNS no arquivo `/etc/resolv.conf`, reinicie a rede e verifique se tudo está funcionando:

```
# hostname
LinServer-A

# whoami
root

# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto eth0

iface eth0 inet static
address 172.16.1.10
netmask 255.255.255.0
gateway 172.16.1.1

# cat /etc/resolv.conf
nameserver 8.8.8.8
nameserver 8.8.4.4

# systemctl restart networking

# ip a s | grep '^ *inet '
    inet 127.0.0.1/8 scope host lo
    inet 172.16.1.10/24 brd 172.16.1.255 scope global eth0
```

4. Vamos para a máquina *WinServer-G*. Assim que a máquina terminar de ligar, clique em `OK` para entrar com uma nova senha, e informe a senha `rnpesr`. Na próxima tela, escolha "*Activate Later*".

   Pelo *Control Panel* ou usando o comando `ncpa.cpl`, configure o endereço IP e servidores DNS de forma estática, como na foto abaixo, e verifique que suas configurações estão funcionais.

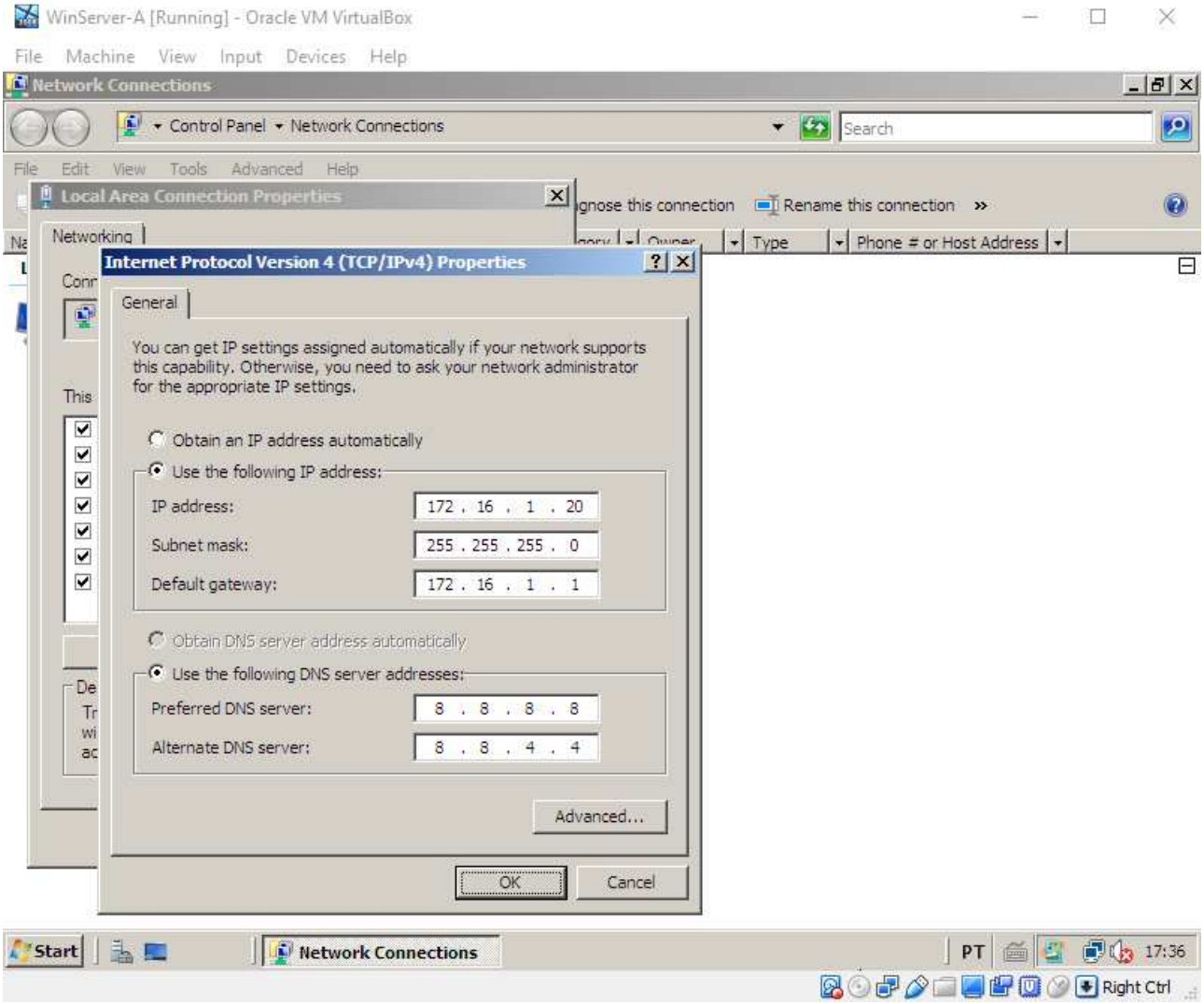

Figura 2: Configuração de rede da máquina WinServer-G

5. Prossiga para a máquina *KaliLinux-G*, e faça login como usuário `root` e senha `rnpesr`. Se tiver problemas com o mapa de teclado, abra um terminal e digite:

```
# gnome-control-center region
```

   Em *Input Sources*, clique no botão `+` para adicionar um novo mapa de teclado. Clique no símbolo `⋯` na parte de baixo da nova janela e procure o teclado *Portuguese (Brazil)*. Em seguida, clique em *Add*. Finalmente, apague o teclado original selecionando *English (US)* e clicando no botão `-`.

6. Ainda na máquina *KaliLinux-G*, edite as configurações de rede no arquivo `/etc/network/interfaces` e de DNS no arquivo `/etc/resolv.conf`. Reinicie a rede e verifique se tudo está funcionando:

```
# hostname
kali

# whoami
root

# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 172.16.1.30
netmask 255.255.255.0
gateway 172.16.1.1

# cat /etc/resolv.conf
nameserver 8.8.8.8
nameserver 8.8.4.4

# ip a s | grep '^ *inet '
    inet 127.0.0.1/8 scope host lo
    inet 172.16.1.30/24 brd 172.16.1.255 scope global eth0
```

7. Finalmente, vamos configurar a máquina *WinClient-G*: faça login como usuário `aluno` e senha `rnpesr`. Acesse o *Control Panel* ou use o comando `ncpa.cpl`, configure o endereço IP e servidores DNS de forma estática, como na foto abaixo, e verifique que suas configurações estão funcionais.

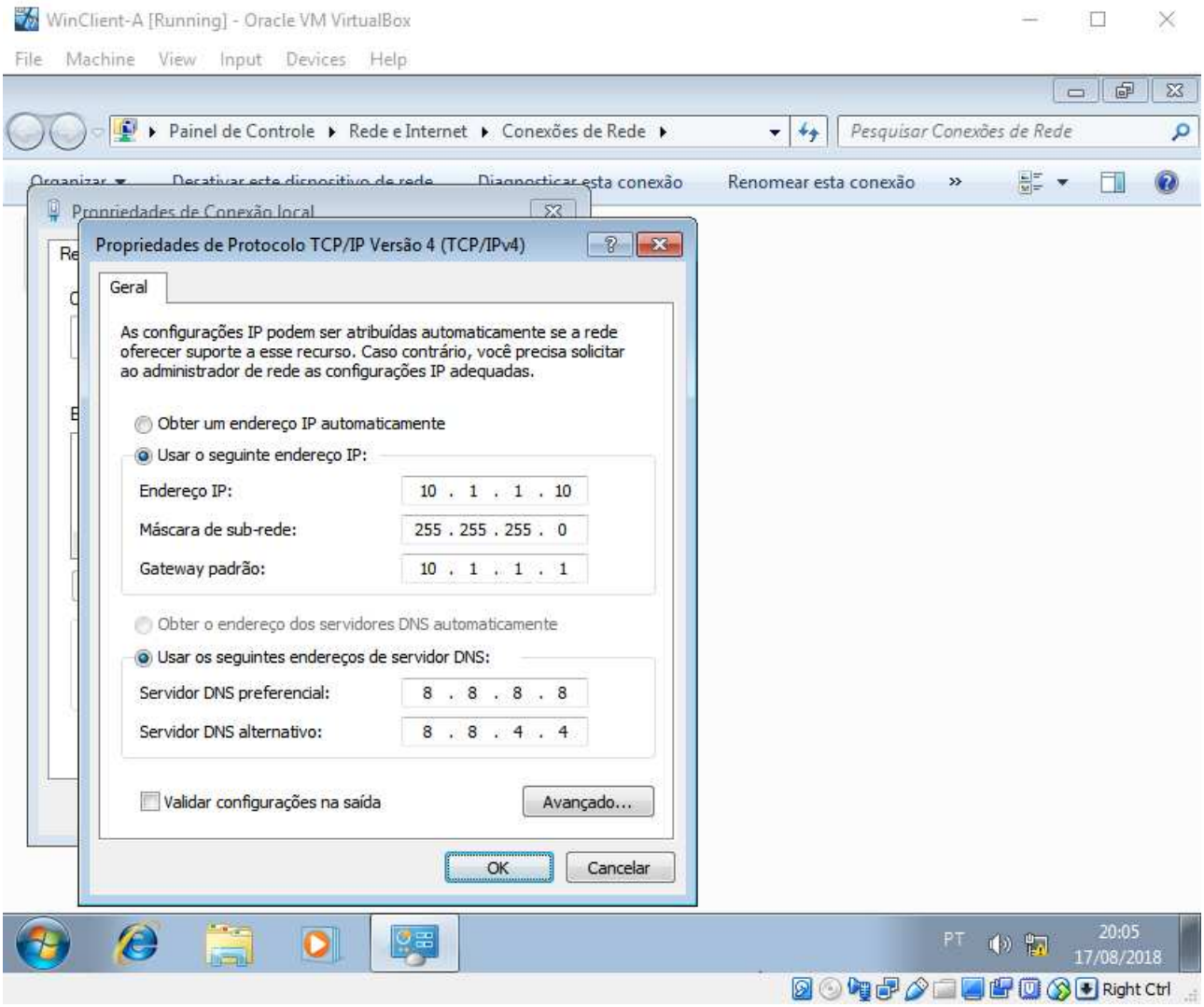

Figura 3: Configuração de rede da máquina WinClient-G

6) Configuração de firewall e NAT

O passo final é garantir que as VMs consigam acessar a internet através da máquina *FWGW1-G*, que é o firewall/roteador na topologia de rede do curso.

1. Antes de mais nada, observe que na máquina *FWGW1-G* já existe uma configuração de *masquerading* (um tipo de SNAT que veremos em maior detalhe na sessão 5) no arquivo `/etc/rc.local`:

```
# hostname
FWGW1-A

# cat /etc/rc.local | grep -v '^#'
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
exit 0
```

2. Isto significa dizer que a tradução de endereços das redes privadas já está configurado. Basta, então, habilitar o repasse de pacotes entre interfaces — descomente a linha `net.ipv4.ip_forward=1` no arquivo `/etc/sysctl.conf` e, posteriormente, execute `# sysctl -p`:

```
# sed -i 's/^#\(net.ipv4.ip_forward\)/\1/' /etc/sysctl.conf

# grep 'net.ipv4.ip_forward' /etc/sysctl.conf
net.ipv4.ip_forward=1

# sysctl -p
net.ipv4.ip_forward = 1
```

3. Finalmente, habilite IP *masquerading* no firewall através do comando `# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`:

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# iptables -L POSTROUTING -vn -t nat
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
```

4. Para testar a conectividade, acesse a máquina *LinServer-G* e verifique — você deve conseguir `ping` com um *host* da internet, como `8.8.8.8`, por exemplo:

```
$ ping -c3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=30.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=31.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=30.9 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 30.916/31.084/31.388/0.296 ms
```

7) Instalação do *Virtualbox Guest Additions* nas VMs Windows

Vamos agora instalar os adicionais de convidado para máquinas virtuais do Virtualbox, conhecido como *Virtualbox Guest Additions*. Esse adicionais consistem em *drivers* de dispositivo e aplicações de sistema que otimizam o sistema para rodar no ambiente virtual, proporcionando maior performance e estabilidade. Nesta atividade, iremos instalar os adicionais apenas nas máquinas *WinServer-G* e *WinClient-G*.

1. Na console da máquina *WinServer-G*, acesse o menu *Devices* > *Insert Guest Additions CD image*. Após algum tempo, a janela de *autorun* irá aparecer, como mostrado abaixo. Clique duas vezes na opção *Run VBoxWindowsAdditions.exe*.

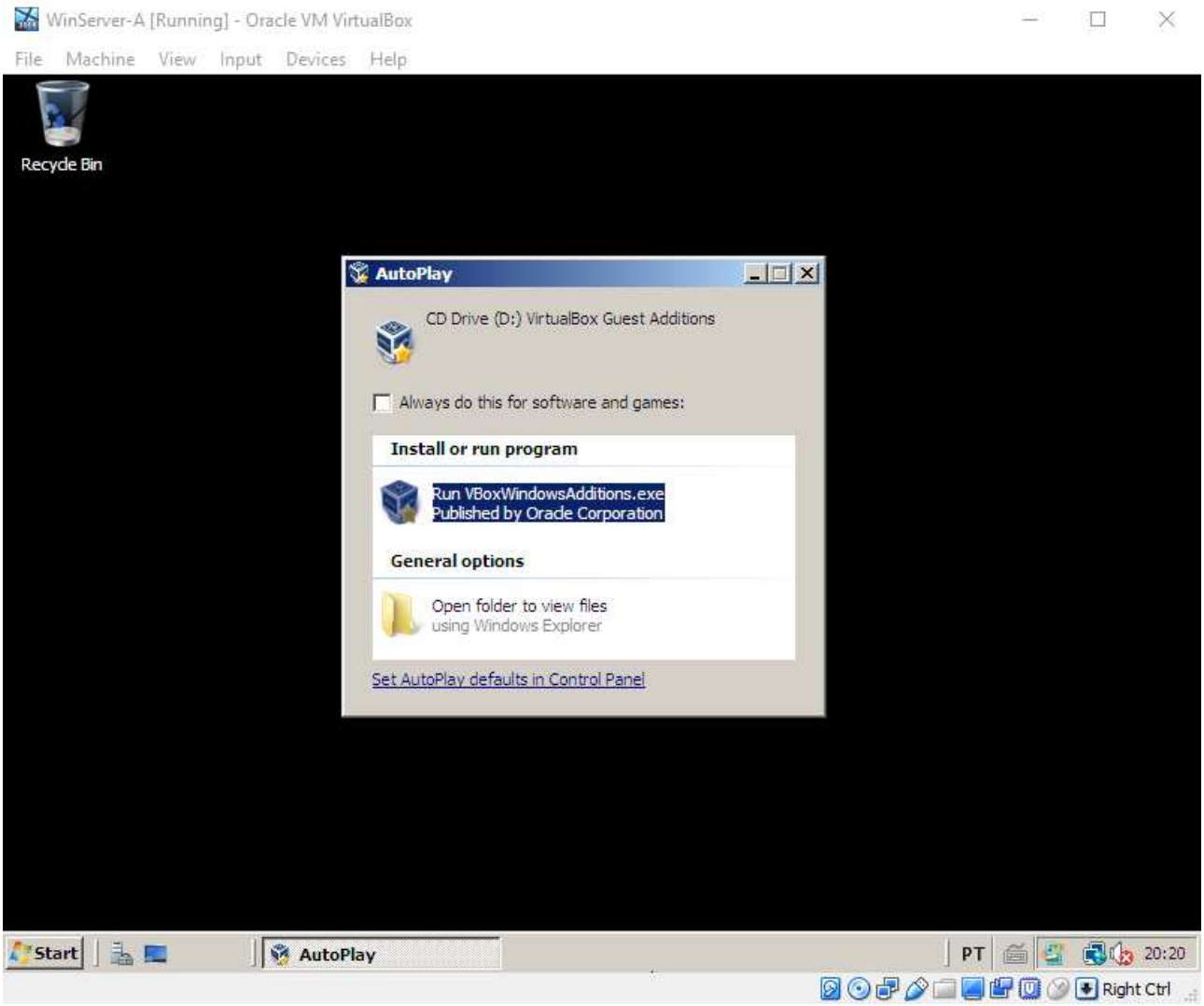

Figura 4: Janela de autorun do CD Virtualbox Guest Additions

2. No assistente de instalação, clique em *Next*, *Next*, e finalmente em *Install*. No meio da instalação o sistema irá avisar que a assinatura de quem publicou o software não é conhecida. Clique em *Install this driver software anyway*, como mostrado abaixo. A mesma janela irá aparecer logo depois, então escolha a mesma opção.

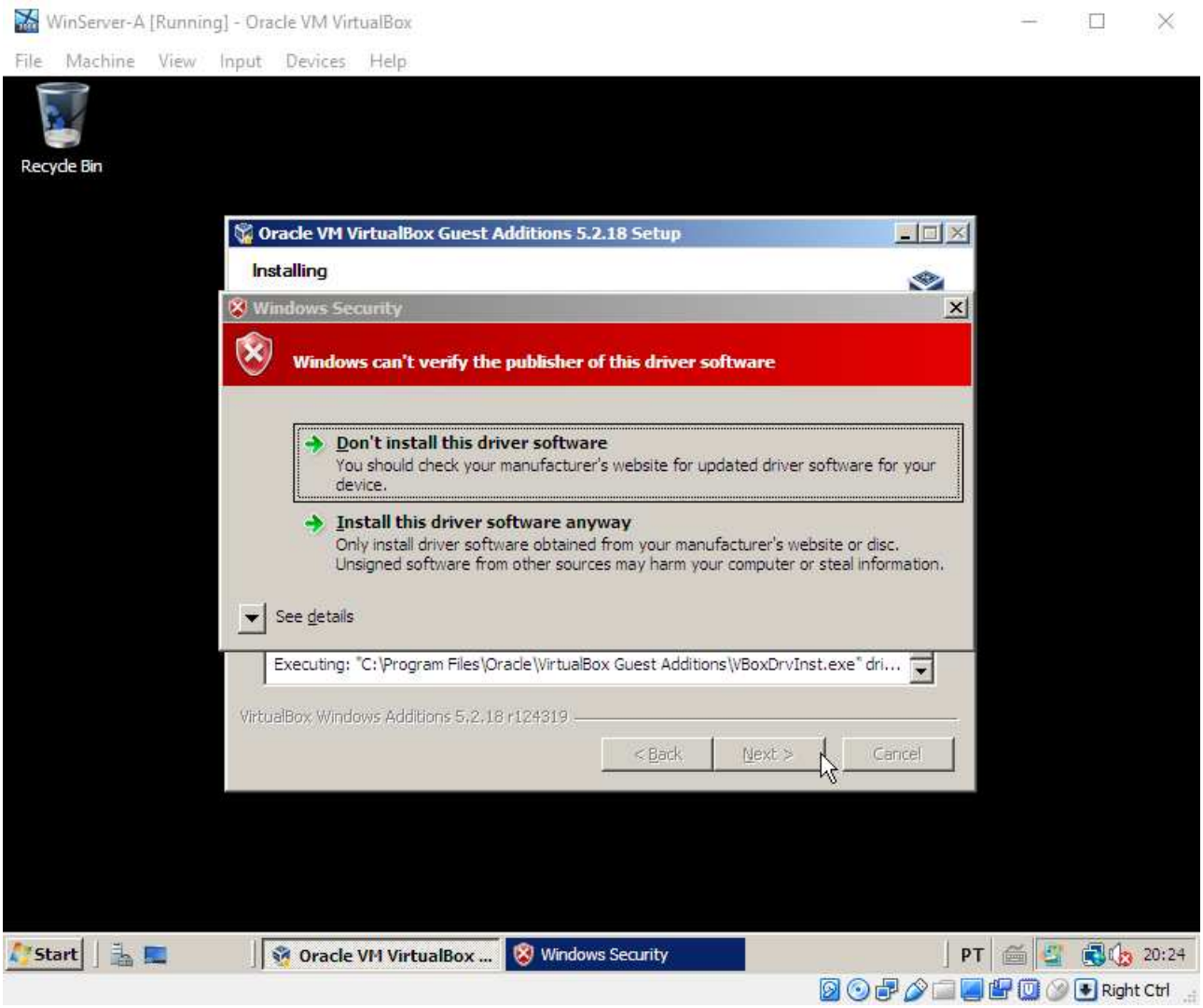

Figura 5: Aviso de publisher não verificado do Virtualbox Guest Additions

3. Ao final da instalação, o assistente irá solicitar que o computador seja reiniciado. Deixe a caixa *Reboot now* marcada e clique em *Finish*.
4. Após o reinício do sistema, maximize a janela do Virtualbox e faça login no sistema como o usuário `Administrator`. Observe que, agora, o *desktop* do Windows Server 2008 ocupa toda extensão do monitor, e não apenas uma pequena janela — indício de que a instalação do *Virtualbox Guest Additions* foi realizada com sucesso.
5. Repita o procedimento de instalação dos passos 1 - 4 na máquina *WinClient-G*.

8) Instalação do *Virtualbox Guest Additions* nas VMs Linux

A instalação do *Virtualbox Guest Additions* nas VMs Linux é um pouco diferente, mais manual. Siga os passos a seguir:

1. Vamos começar pela máquina *FWGW1-G*. Primeiro, faça login como `root` e edite o arquivo `/etc/apt/sources.list` com o seguinte conteúdo:

```
# cat /etc/apt/sources.list
deb http://ftp.br.debian.org/debian/ jessie         main contrib non-free
deb http://ftp.br.debian.org/debian/ jessie-updates main contrib non-free
deb http://security.debian.org/      jessie/updates main contrib non-free
```

2. Em seguida, atualize os repositórios com o comando `apt-get update` e depois instale os pacotes `build-essential` e `module-assistant`, sem incluir recomendações:

```
# apt-get update
# apt-get install --no-install-recommends build-essential module-assistant
```

3. Agora, faça o download dos `headers` do kernel em execução no sistema:

```
# m-a prepare
```

4. Na console do Virtualbox da máquina *FWGW1-G*, acesse o menu *Devices* > *Insert Guest Additions CD image*. Em seguida, monte o dispositivo:

```
# mount /dev/cdrom /mnt/
```

5. Agora, execute o instalador do *Virtualbox Guest Additions*, com o comando:

```
# sh /mnt/VBoxLinuxAdditions.run
Verifying archive integrity... All good.
Uncompressing VirtualBox 5.2.18 Guest Additions for Linux........
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
VirtualBox Guest Additions: Building the VirtualBox Guest Additions kernel modules.
This may take a while.
VirtualBox Guest Additions: Starting.
```

6. Finalmente, reinicie a máquina. Após o *reboot*, verifique que os módulos do *Virtualbox Guest Additions* estão operacionais:

```
# reboot

(...)

# lsmod | grep '^vbox'
vboxsf                 36413  0
vboxvideo              34226  1
vboxguest             221732  2 vboxsf
```

7. Instale os módulos do *Virtualbox Guest Additions* na máquina *LinServer-G*. O procedimento é idêntico ao que fizemos nos passos 1 - 6.

Não iremos instalar os módulos do *Virtualbox Guest Additions* na máquina *KaliLinux-G*. Pelo fato de a VM estar um pouco desatualizada (jan/2016), o `apt` exige que um grande número de pacotes seja baixado antes que os *headers* do kernel possam ser recuperados. Visto que o tempo de instalação e download desses pacotes é longo, vamos pular essa etapa.

Não obstante, os passos de instalação são idênticos aos das máquinas *FWGW1-G* e *LinServer-G*. O Kali Linux é baseado na distribuição Debian, que está sendo usado nessas duas VMs.

9) Configuração da VM *WinServer-G*

A máquina *WinServer-G* demanda uma pequena configuração adicional antes que estejamos prontos para começar os trabalhos. Vamos a ela:

1. Usando o 1) *Control Panel*, 2) clique direito em *Computer* > *Properties* no Windows Explorer ou 3) digitando `system` no menu iniciar, abra a tela de configuração do sistema como mostrado a seguir:

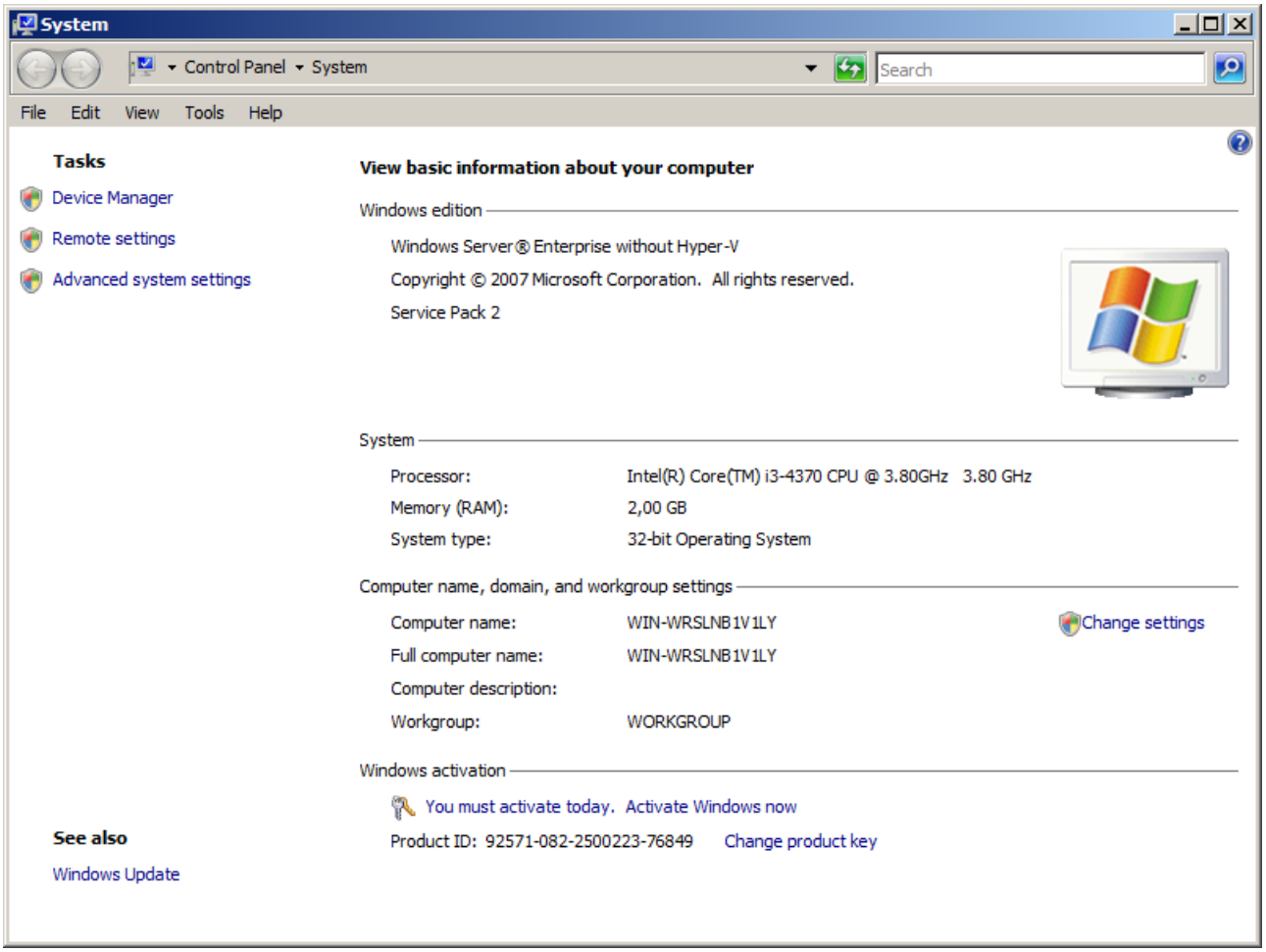

Figura 6: Tela de configuração do sistema do WinServer

2. Clique em *Change Settings*, e na aba *Computer Name*, no botão *Change...*. Altere o nome do computador para `WinServer-G` e o *Workgroup* para `GRUPO`, como se segue. Depois, clique em *OK*.

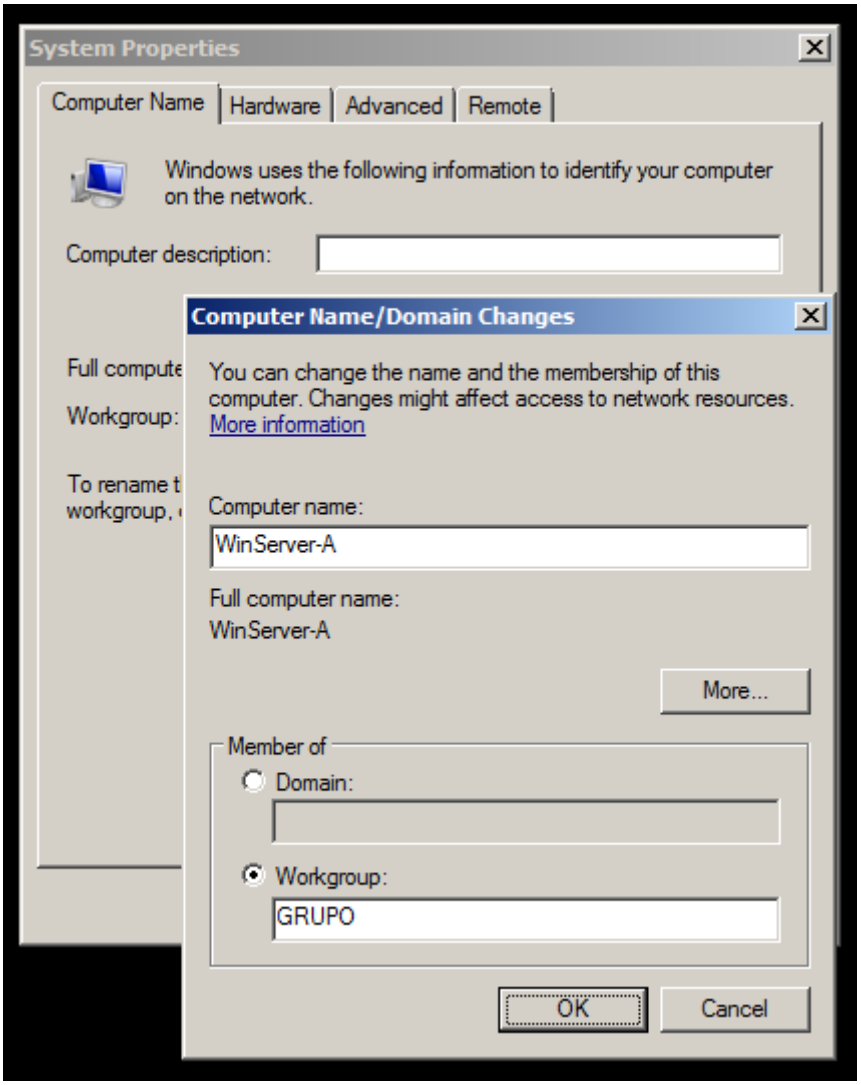

Figura 7: Alteração de nome de máquina do WinServer

3. Não reinicie o computador ainda. Na aba *Remote*, marque a caixa *Allow Connections from computers running any version of Remote Desktop (less secure)*. Depois, clique em *Apply* e em seguida em *Restart Later*.

4. Agora, desabilite o firewall do Windows. Digite `firewall` no menu *Start* (alternativamente, clique em *Windows Firewall* no *Control Panel*), em seguida em *Turn Windows Firewall on or off*, e finalmente marque a caixa *Off*, como se segue:

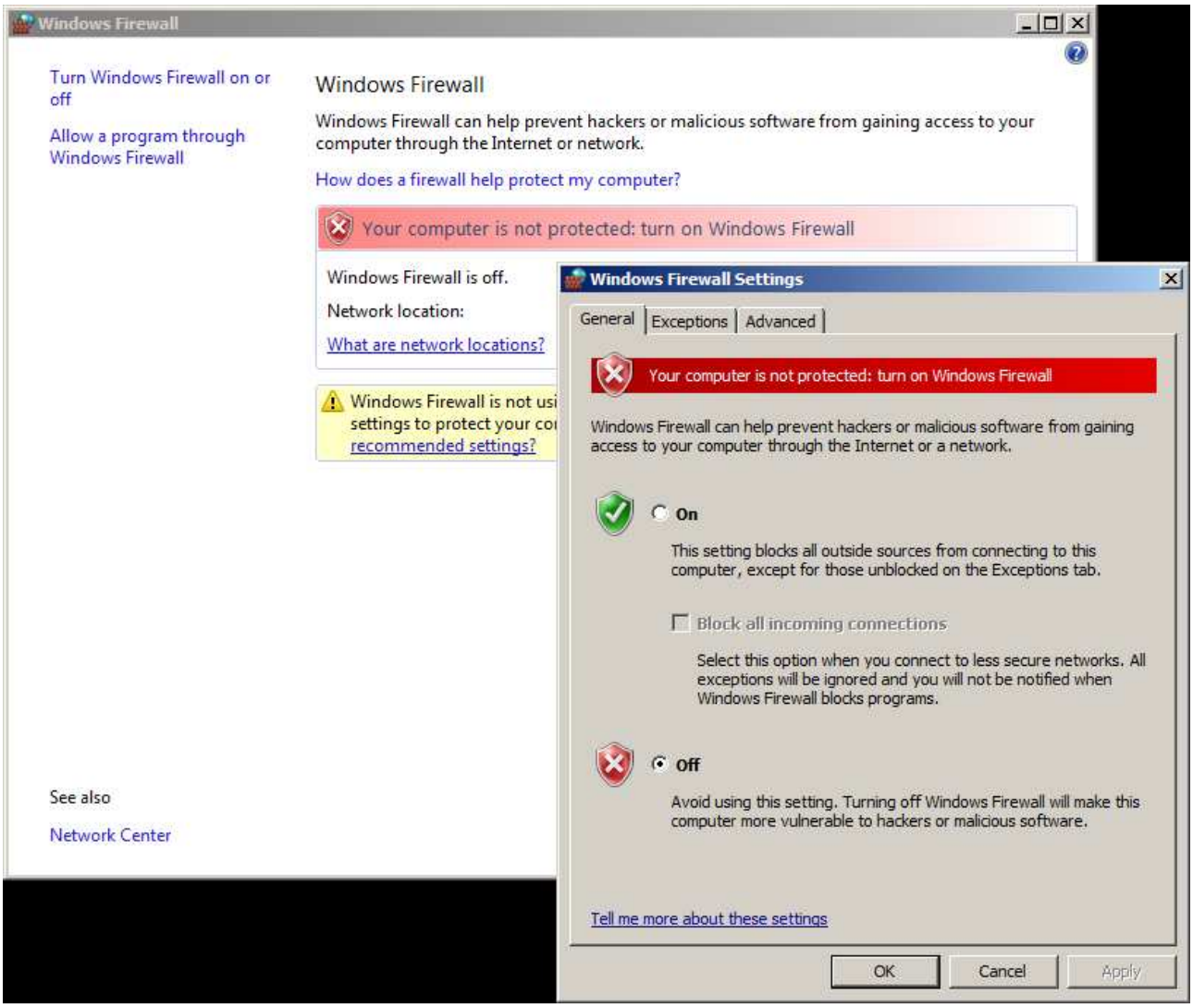

Figura 8: Desabilitar o firewall do WinServer

5. Clique em *OK* e reinicie a máquina *WinServer-G*.

6. Após o *reboot*, abra o *Server Manager* (é o primeiro ícone à direta do botão *Start*), e em seguida clique com o botão direito em *Roles*, selecionando *Add Roles*. Na janela subsequente, clique em *Next*. Depois, marque a caixa da *role Web Server (IIS)*, como se segue. Quando surgir a pergunta *Add features required for Web Server (IIS)?*, clique em *Add Required Features*, e depois em *Next*.

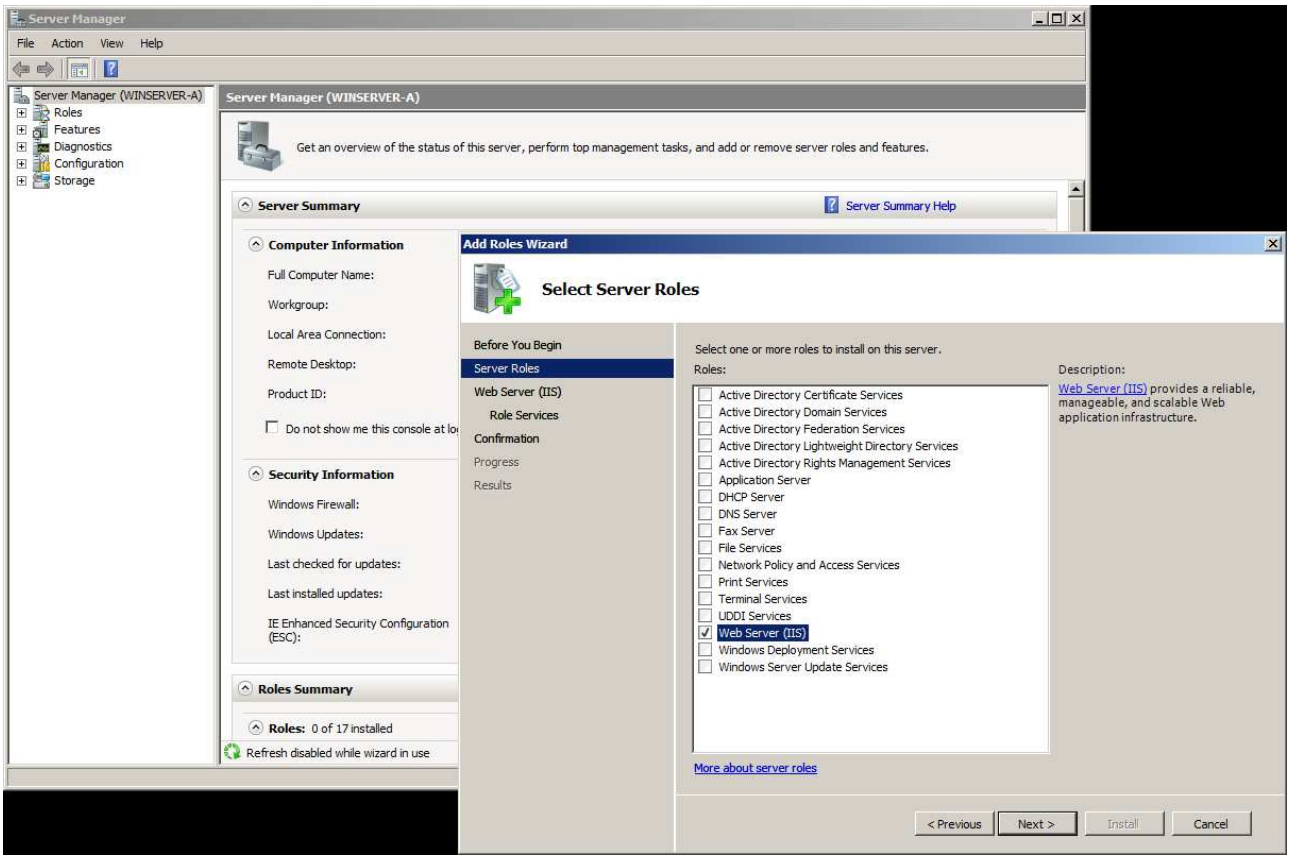

Figura 9: Instalando a role IIS no WinServer

7. Na janela *Introduction to Web Server (IIS)*, clique em *Next*. A seguir, na janela *Role services*, desça a barra de rolagem até o final e marque a caixa *FTP Publishing Service*, como se segue. Da mesma forma que antes, quando surgir a pergunta *Add features required for FTP Publishing Service?*, clique em *Add Required Features*, e depois em *Next*.

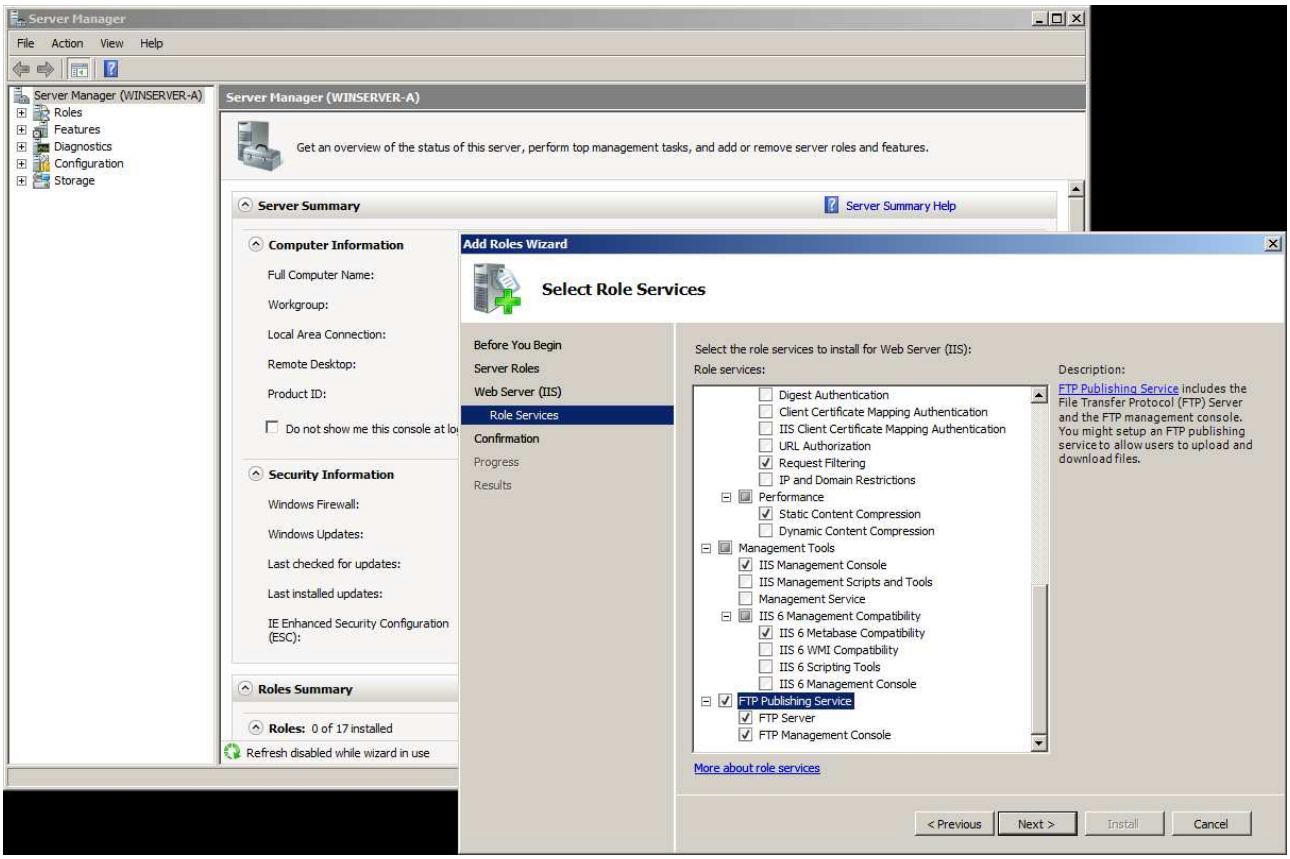

Figura 10: Instalando a feature FTP Server no WinServer

8. Finalmente, clique em *Install* e aguarde. Ao final do processo, clique em *Close*.

Sessão 2: Conceitos fundamentais em segurança da informação

1) Listas e informações complementares de segurança

1. Visite e assine a lista de e-mail do CAIS/RNP:
   - https://memoria.rnp.br/cais/listas.php
2. Visite e assine as listas de algumas das instituições mais respeitadas sobre segurança no mundo:
   - http://www.securityfocus.com/archive/
   - http://www.sans.org/newsletters/
   - https://www.us-cert.gov/mailing-lists-and-feeds
   - http://seclists.org/

   Você é capaz de dizer em poucas palavras a diferença entre as listas assinadas, principalmente no foco de abordagem?
3. O Cert.br disponibiliza uma cartilha com informações sobre segurança na internet através do link https://cartilha.cert.br/. Acesse o fascículo “Segurança na internet”. Você consegue listar quais são os riscos a que estamos expostos com o uso da internet, e como podemos nos prevenir?
4. Veja os vídeos educativos sobre segurança do NIC.BR em http://antispam.br/videos/. Em seguida, pesquise na Internet e indique um exemplo relevante de cada categoria:
   - Vírus
   - Worms
   - Cavalos de troia (*trojan horses*)
   - Spyware
   - Bot
   - Engenharia social
   - *Phishing*
5. O site http://www.antispam.br/admin/porta25/ apresenta um conjunto de políticas e padrões chamados de “Gerência de Porta 25”, que podem ser utilizados em redes de usuários finais ou de caráter residencial para:
   - Mitigar o abuso de proxies abertos e máquinas infectadas para o envio de spam.
   - Aumentar a rastreabilidade de fraudadores e spammers.

   Estude no que consiste e quais são os benefícios da gerência da porta 25, e responda: sua instituição tem políticas de mitigação para os riscos apresentados? Quais seriam boas medidas operacionais para detectar e solucionar problemas relacionados à porta 25?

2) Segurança física e lógica

1. Delineie, de forma sucinta, qual seria seu plano de segurança para uma empresa em cada um dos tópicos abaixo:
    - Contenção de catástrofes.
    - Proteção das informações (backup).
    - Controle de acesso.
    - Garantia de fornecimento de energia.
    - Redundância.
2. Quantos níveis de segurança possui a rede da sua instituição? Quais são? Faça um desenho da topologia da solução.
3. Cite 5 controles que podemos utilizar para aumentar a segurança física de um ambiente.
4. Cite 5 controles que podemos utilizar para aumentar a segurança lógica de um ambiente.
5. Informe em cada círculo dos diagramas seguintes o equipamento correto para a rede, através dos números indicados a seguir, que proporcione um nível de segurança satisfatório. Justifique suas respostas.

    1. IDS
    2. Modem
    3. Firewall
    4. Proxy
    5. Switch
    6. Roteador