Fatec São Caetano do Sul Antonio Russo

Centro Paula Souza

GOVERNO DO ESTADO DE SÃO PAULO

CURSO: Segurança da Informação

DISCIPLINA	Laboratório de Administração de Sistemas Operacionais de Redes (SEGMA3)			**PROFESSOR (A)**	Ms. Claudio Cura Jr		
ALUNO (A) Nome completo	Enzo Arrue Juan Fuso					**RA**	
CICLO (SEMESTRE)	3	**TURNO**	**Matutino**	**DATA**	29/04/2025	**NOTA**	
ATV: Ataque DDoS							

Atividade prática “DDoS / Ping da Morte”:

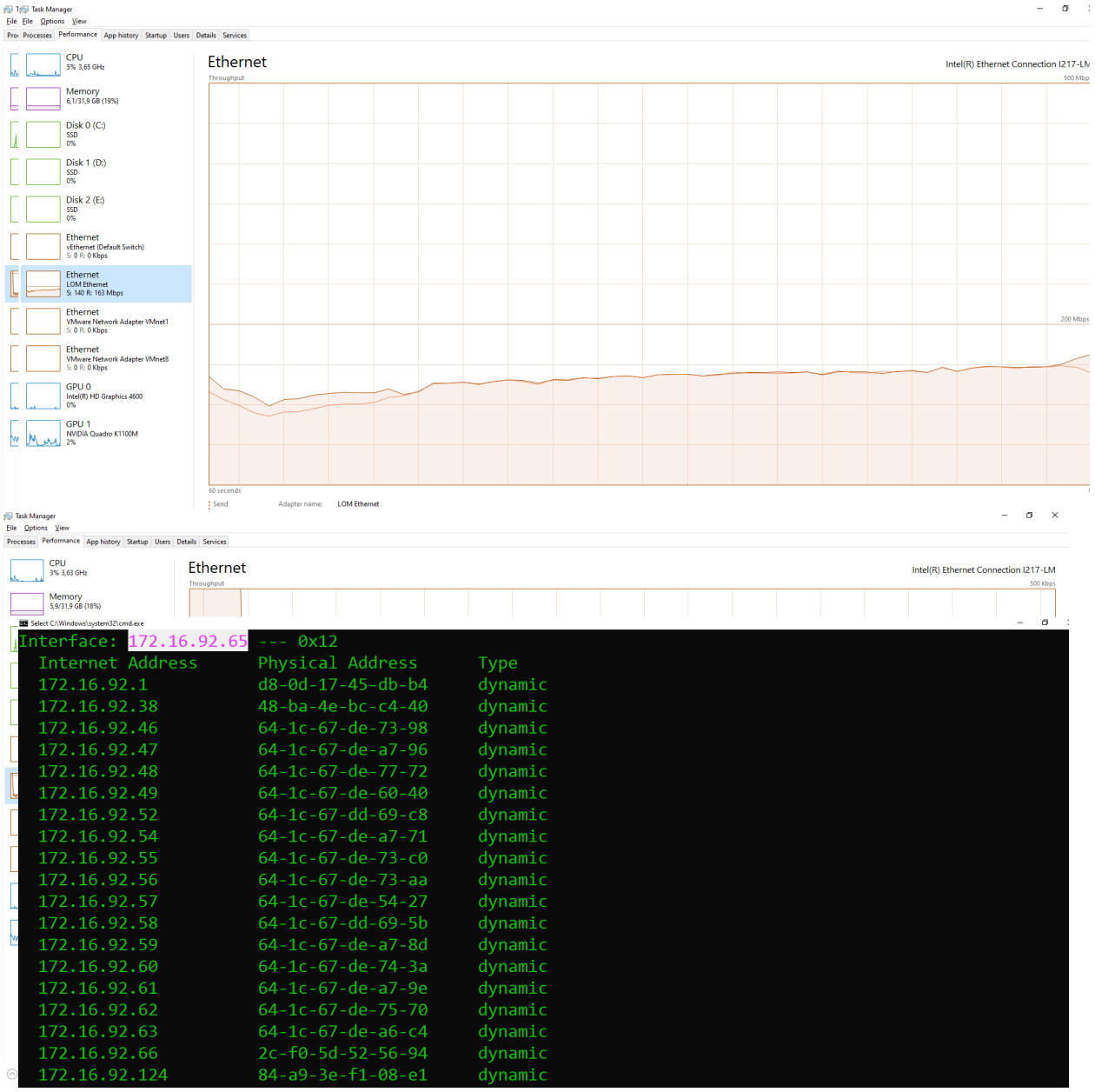
Na aula prática realizada em 13 de maio de 2025, tivemos a oportunidade de simular um ataque de negação de serviço distribuído (DDoS) com o intuito de compreender melhor seu funcionamento e seus impactos em redes e sistemas. A atividade teve como principal objetivo demonstrar, de forma prática, como esse tipo de ataque pode sobrecarregar um dispositivo ou serviço, tornando-o inoperante.
Para que o experimento fosse executado corretamente, foi necessário desativar o firewall tanto em nossas máquinas quanto no computador do professor, que serviu como alvo da simulação. O firewall é um mecanismo essencial de proteção, responsável por filtrar conexões indesejadas e impedir acessos não autorizados. Portanto, sua desativação temporária foi imprescindível para permitir o recebimento irrestrito dos pacotes de dados durante o teste.

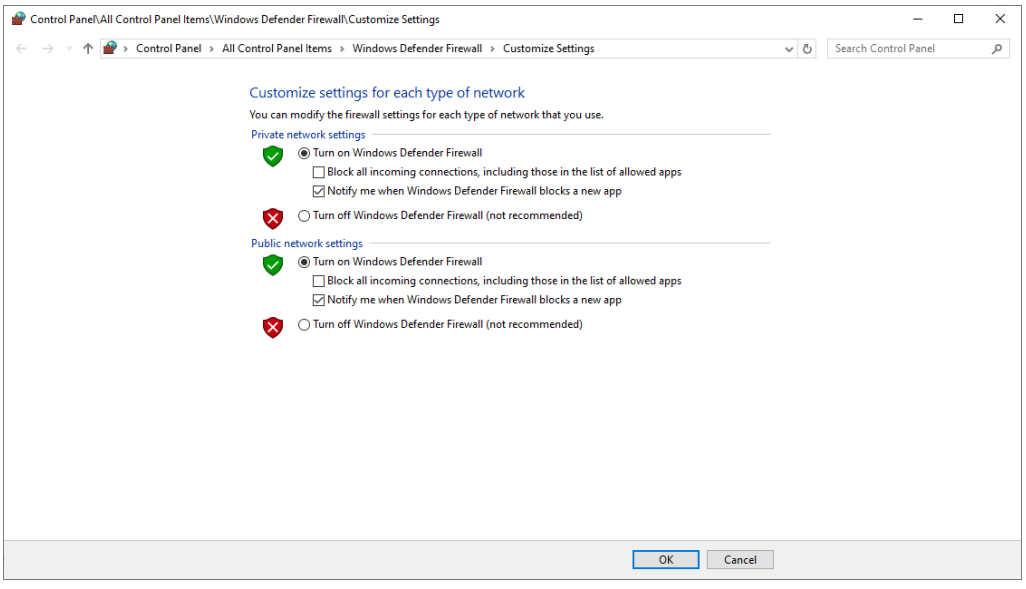
Utilizando o prompt de comando do Windows (cmd), executamos múltiplos envios de pacotes ICMP por meio do comando ping [IP] -t. Esse comando força o envio contínuo de pings ao endereço de destino até que seja interrompido manualmente. Iniciamos com um número reduzido de requisições e, gradualmente, aumentamos a quantidade até atingir aproximadamente 65.000 pacotes enviados. À medida que mais estudantes executavam o mesmo comando simultaneamente, o computador do professor passou a processar um grande volume de requisições em tempo real, simulando com fidelidade o cenário de um ataque DDoS.

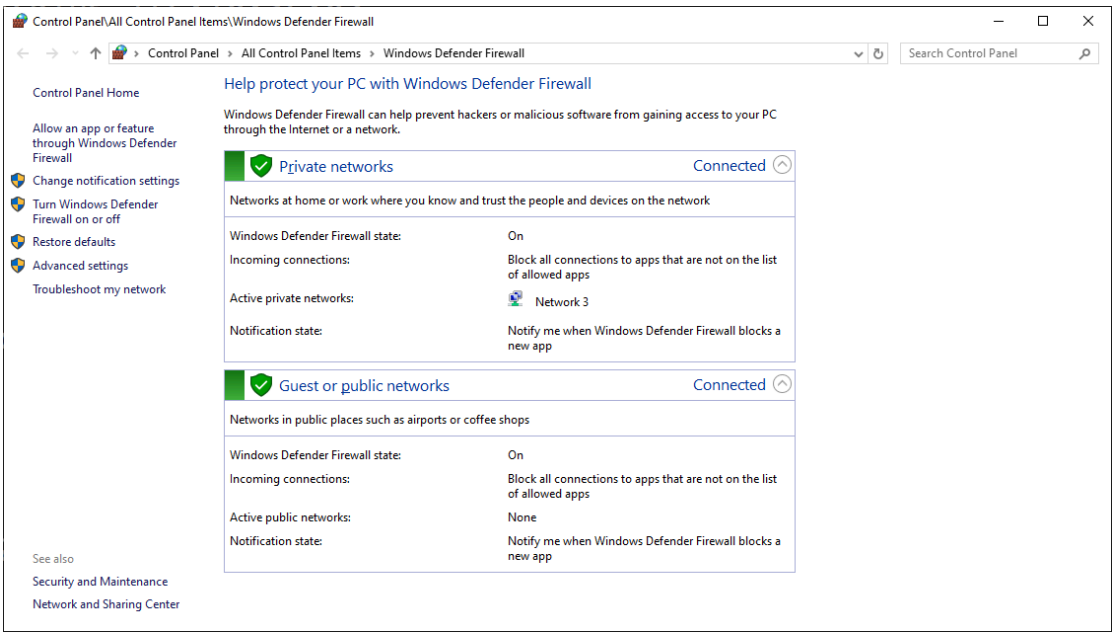
Como consequência, a máquina-alvo começou a apresentar lentidão na resposta e, eventualmente, falhas temporárias de conectividade, evidenciando os efeitos de uma sobrecarga na rede. A experiência permitiu visualizar na prática a vulnerabilidade dos sistemas diante desse tipo de ataque e reforçou a importância de implementar medidas de segurança eficazes, como a manutenção adequada de firewalls e outros mecanismos de defesa.

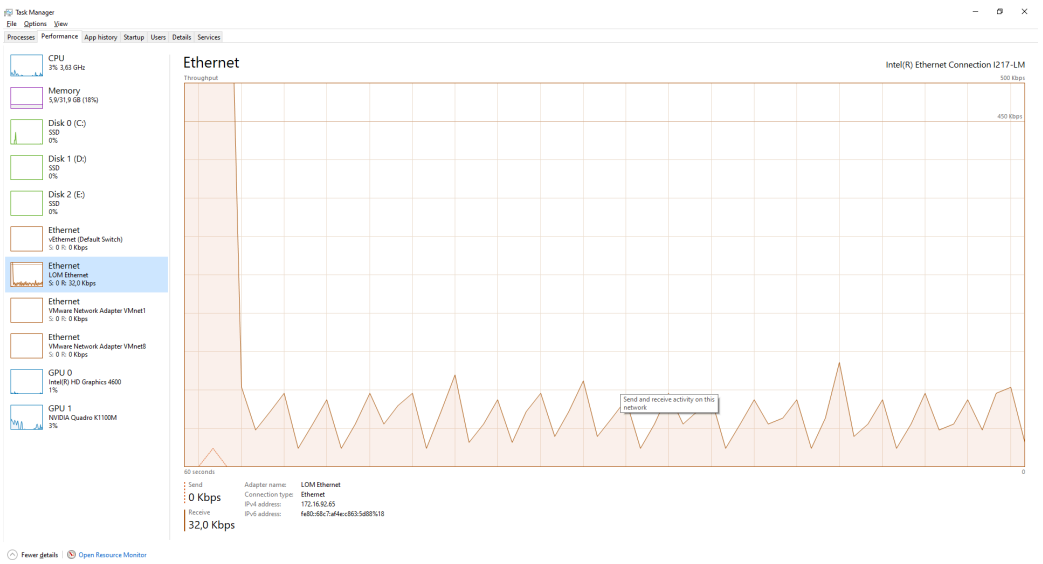
Essa aula prática foi fundamental para consolidar nosso entendimento sobre segurança da informação, ao ilustrar de maneira concreta os perigos associados a ataques cibernéticos e a necessidade de proteção contra eles.

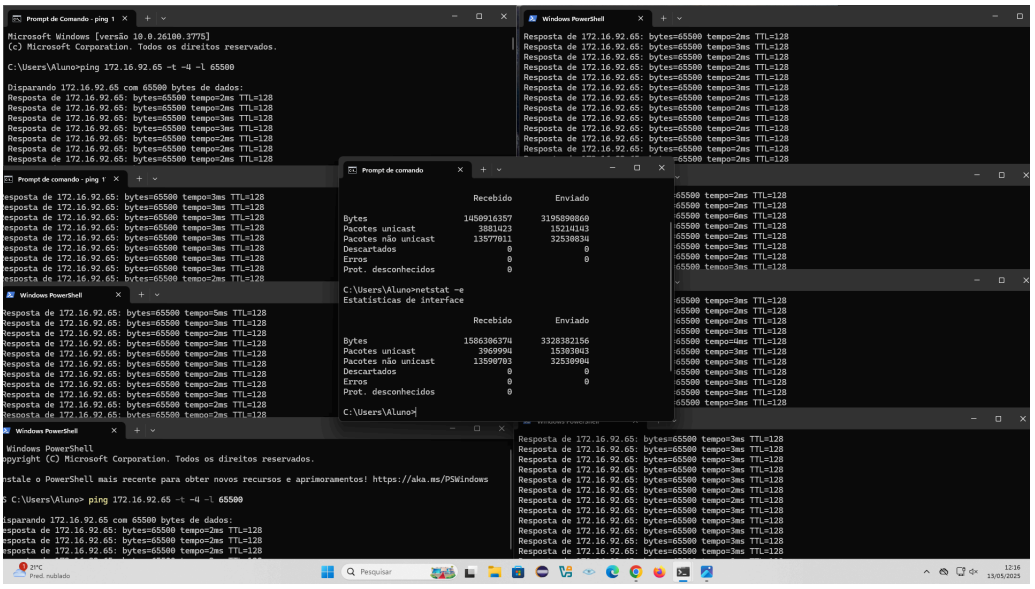
PRINTS:

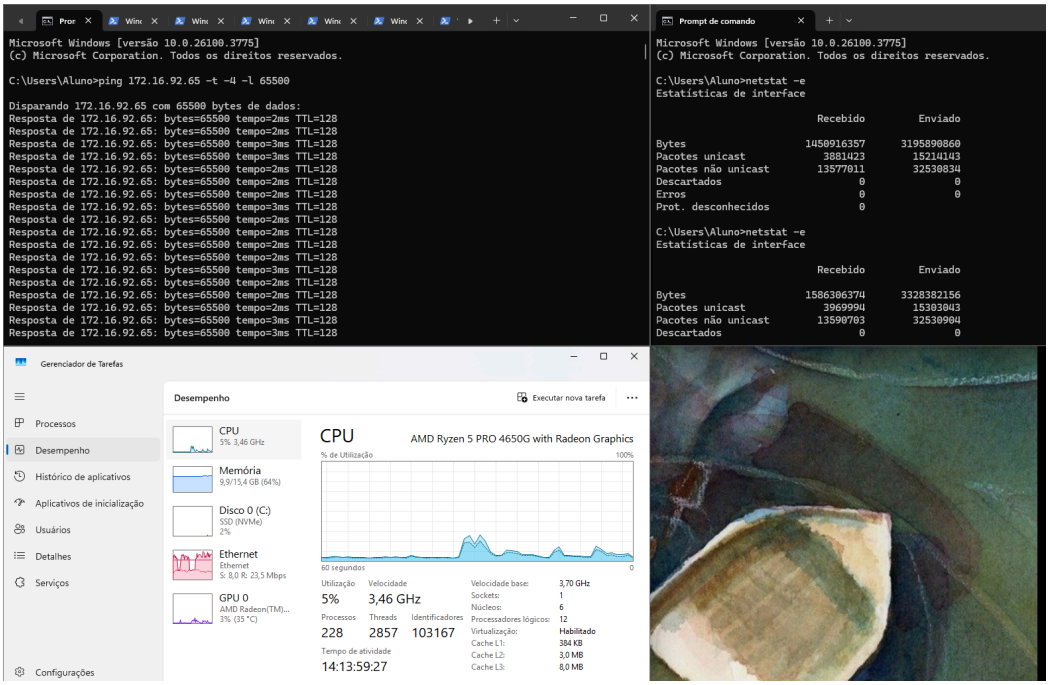

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
5% 3,65 GHz
Memory
6,1/31,9 GB (19%)
Disk 0 (C:)
SSD
0%
Disk 1 (D:)
SSD
0%
Disk 2 (E:)
SSD
0%
Ethernet
vEthernet (Default Switch)
S: 0 R: 0 Kbps
Ethernet
LOM Ethernet
S: 140 R: 163 Mbps
Ethernet
VMware Network Adapter VMnet1
S: 0 R: 0 Kbps
Ethernet
VMware Network Adapter VMnet8
S: 0 R: 0 Kbps
GPU 0
Intel(R) HD Graphics 4600
0%
GPU 1
NVIDIA Quadro K1100M
2%
Ethernet
Intel(R) Ethernet Connection I217-LM
Throughput
500 Mbps
200 Mbps
60 seconds
Send
Adapter name: LOM Ethernet
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
3% 3,63 GHz
Memory
5,9/31,9 GB (18%)
Ethernet
Intel(R) Ethernet Connection I217-LM
Throughput
500 Kbps
Select C:\Windows\system32\cmd.exe
Interface: 172.16.92.65 --- 0x12
Internet Address Physical Address Type
172.16.92.1 d8-0d-17-45-db-b4 dynamic
172.16.92.38 48-ba-4e-bc-c4-40 dynamic
172.16.92.46 64-1c-67-de-73-98 dynamic
172.16.92.47 64-1c-67-de-a7-96 dynamic
172.16.92.48 64-1c-67-de-77-72 dynamic
172.16.92.49 64-1c-67-de-60-40 dynamic
172.16.92.52 64-1c-67-dd-69-c8 dynamic
172.16.92.54 64-1c-67-de-a7-71 dynamic
172.16.92.55 64-1c-67-de-73-c0 dynamic
172.16.92.56 64-1c-67-de-73-aa dynamic
172.16.92.57 64-1c-67-de-54-27 dynamic
172.16.92.58 64-1c-67-dd-69-5b dynamic
172.16.92.59 64-1c-67-de-a7-8d dynamic
172.16.92.60 64-1c-67-de-74-3a dynamic
172.16.92.61 64-1c-67-de-a7-9e dynamic
172.16.92.62 64-1c-67-de-75-70 dynamic
172.16.92.63 64-1c-67-de-a6-c4 dynamic
172.16.92.66 2c-f0-5d-52-56-94 dynamic
172.16.92.124 84-a9-3e-f1-08-e1 dynamic

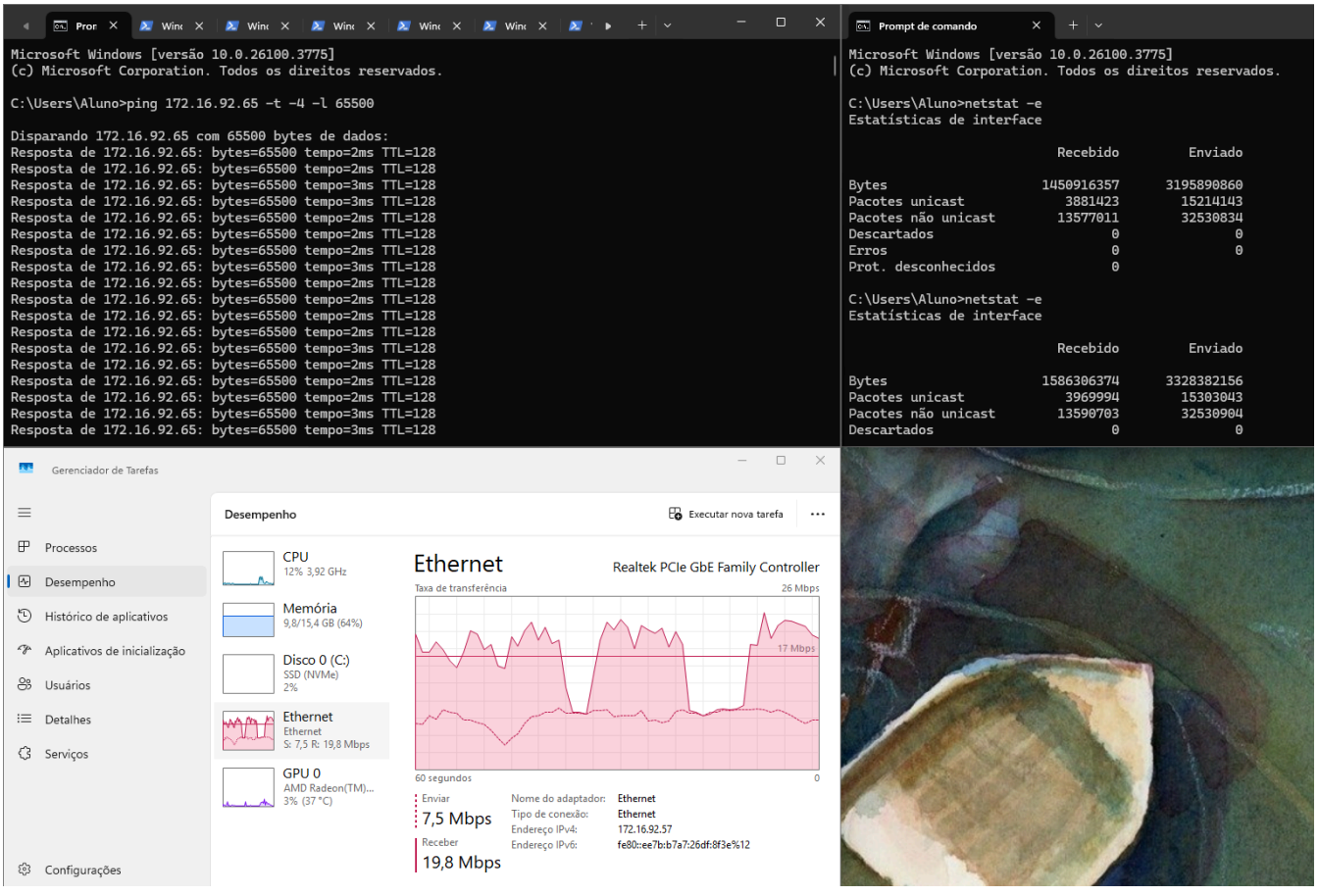

Control Panel\All Control Panel Items\Windows Defender Firewall\Customize Settings
Control Panel › All Control Panel Items › Windows Defender Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Public network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
OK
Cancel

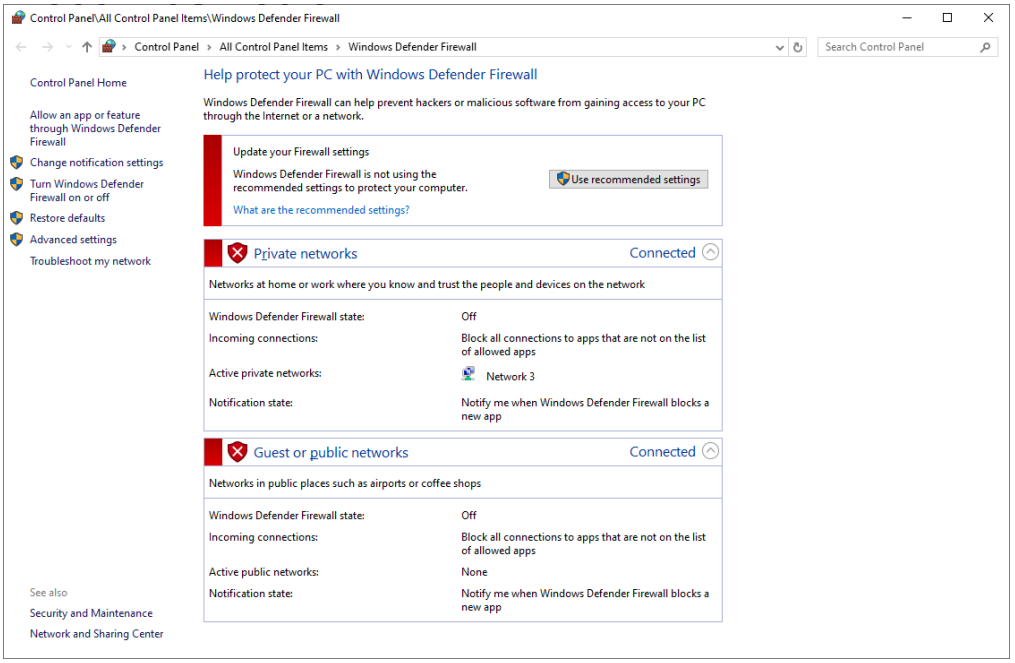

Control Panel\All Control Panel Items\Windows Defender Firewall
Control Panel › All Control Panel Items › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Private networks
Connected
Networks at home or work where you know and trust the people and devices on the network
Windows Defender Firewall state: On
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active private networks: Network 3
Notification state: Notify me when Windows Defender Firewall blocks a new app
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Defender Firewall state: On
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active public networks: None
Notification state: Notify me when Windows Defender Firewall blocks a new app
See also
Security and Maintenance
Network and Sharing Center


Task Manager
Ethernet
Intel(R) Ethernet Connection I217-LM
0 Kbps
32,0 Kbps


Prompt de Comando - ping 1
Microsoft Windows [versão 10.0.26100.3775]
(c) Microsoft Corporation. Todos os direitos reservados.
C:\Users\Aluno>ping 172.16.92.65 -t -4 -l 65500
Disparando 172.16.92.65 com 65500 bytes de dados:
Windows PowerShell
Prompt de comando
Recebido Enviado
Bytes 1458916357 3195890860
Pacotes unicast 3881423 15214143
Pacotes não unicast 13577011 32530834
Descartados 0 0
Erros 0 0
Prot. desconhecidos 0
C:\Users\Aluno>netstat -e
Estatísticas de interface
Recebido Enviado
Bytes 158630637 3328382156
Pacotes unicast 396999 15303043
Pacotes não unicast 13590703 32530904
Descartados 0 0
Erros 0 0
Prot. desconhecidos 0
C:\Users\Aluno>
Windows PowerShell
Instale o PowerShell mais recente para obter novos recursos e aprimoramentos! https://aka.ms/PSWindows
C:\Users\Aluno> ping 172.16.92.65 -t -4 -l 65500


Microsoft Windows [versão 10.0.26100.3775]
(c) Microsoft Corporation. Todos os direitos reservados.
C:\Users\Aluno>ping 172.16.92.65 -t -4 -l 65500
Disparando 172.16.92.65 com 65500 bytes de dados:
Resposta de 172.16.92.65: bytes=65500 tempo=2ms TTL=128
Resposta de 172.16.92.65: bytes=65500 tempo=3ms TTL=128
Prompt de comando
C:\Users\Aluno>netstat -e
Estatísticas de interface
Recebido Enviado
Bytes 1450916357 3195890860
Pacotes unicast 3881423 15214143
Pacotes não unicast 13577011 32530834
Descartados 0 0
Erros 0 0
Prot. desconhecidos 0
C:\Users\Aluno>netstat -e
Estatísticas de interface
Recebido Enviado
Bytes 1586306374 3328382156
Pacotes unicast 3969994 15303043
Pacotes não unicast 13590703 32530904
Descartados 0 0
Gerenciador de Tarefas
Desempenho
Executar nova tarefa
Processos
Desempenho
Histórico de aplicativos
Aplicativos de inicialização
Usuários
Detalhes
Serviços
Configurações
CPU
5% 3,46 GHz
Memória
9,9/15,4 GB (64%)
Disco 0 (C:)
SSD (NVMe)
2%
Ethernet
Ethernet
S: 8,0 R: 23,5 Mbps
GPU 0
AMD Radeon(TM)...
3% (35 °C)
CPU
AMD Ryzen 5 PRO 4650G with Radeon Graphics
% de Utilização
100%
60 segundos
0
Utilização
5%
Velocidade
3,46 GHz
Processos
228
Threads
2857
Identificadores
103167
Tempo de atividade
14:13:59:27
Velocidade base: 3,70 GHz
Sockets: 1
Núcleos: 6
Processadores lógicos: 12
Virtualização: Habilitado
Cache L1: 384 KB
Cache L2: 3,0 MB
Cache L3: 8,0 MB


Microsoft Windows [versão 10.0.26100.3775]
(c) Microsoft Corporation. Todos os direitos reservados.
C:\Users\Aluno>ping 172.16.92.65 -t -4 -l 65500
Disparando 172.16.92.65 com 65500 bytes de dados:
Resposta de 172.16.92.65: bytes=65500 tempo=2ms TTL=128
Resposta de 172.16.92.65: bytes=65500 tempo=3ms TTL=128
Prompt de comando
C:\Users\Aluno>netstat -e
Estatísticas de interface
Recebido Enviado
Bytes 1450916357 3195890860
Pacotes unicast 3881423 15214143
Pacotes não unicast 13577011 32530834
Descartados 0 0
Erros 0 0
Prot. desconhecidos 0
C:\Users\Aluno>netstat -e
Estatísticas de interface
Recebido Enviado
Bytes 1586306374 3328382156
Pacotes unicast 3969994 15303043
Pacotes não unicast 13590703 32530904
Descartados 0 0
Gerenciador de Tarefas
Desempenho
Executar nova tarefa
Processos
Desempenho
Histórico de aplicativos
Aplicativos de inicialização
Usuários
Detalhes
Serviços
Configurações
CPU
12% 3,92 GHz
Memória
9,8/15,4 GB (64%)
Disco 0 (C:)
SSD (NVMe)
2%
Ethernet
Ethernet
S: 7,5 R: 19,8 Mbps
GPU 0
AMD Radeon(TM)...
3% (37 °C)
Ethernet
Realtek PCIe GbE Family Controller
Taxa de transferência
26 Mbps
17 Mbps
60 segundos
0
Enviar
7,5 Mbps
Receber
19,8 Mbps
Nome do adaptador: Ethernet
Tipo de conexão: Ethernet
Endereço IPv4: 172.16.92.57
Endereço IPv6: fe80::ee7b:b7a7:26df:8f3e%12



✅ Questões sobre Ataques DDoS

1. O que caracteriza um ataque DDoS (Distributed Denial of Service)?
D) A sobrecarga de um sistema com requisições vindas de múltiplas fontes.

2. Um dos principais objetivos de um ataque DDoS é:
B) Tornar um serviço ou servidor indisponível.

3. Em um ataque DDoS, o que é comumente usado para gerar o tráfego malicioso?
B) Uma botnet com milhares de dispositivos zumbis.

4. Qual comando pode ser usado no Windows para verificar conexões de rede?
B) netstat

5. Uma maneira de mitigar um ataque DDoS em servidores é:
B) Usar firewall e balanceamento de carga.

6. Qual tipo de ataque DDoS envia pacotes de sincronização TCP repetidamente sem completar a conexão?
C) SYN Flood

7. Em uma rede local, qual comportamento pode indicar um DDoS?
C) Pico súbito de uso de rede sem justificativa.

8. Qual é a principal diferença entre DoS e DDoS?
C) DDoS utiliza múltiplas máquinas; DoS, apenas uma.

9. O que é uma "botnet" no contexto de DDoS?
D) Uma rede de dispositivos comprometidos controlados remotamente.

10. Em uma aula prática de sistemas operacionais, um aluno usa o comando ping 192.168.0.10 -n 1000. Qual o propósito desse comando?

C) Enviar 1000 requisições ICMP consecutivas para o IP 192.168.0.10.