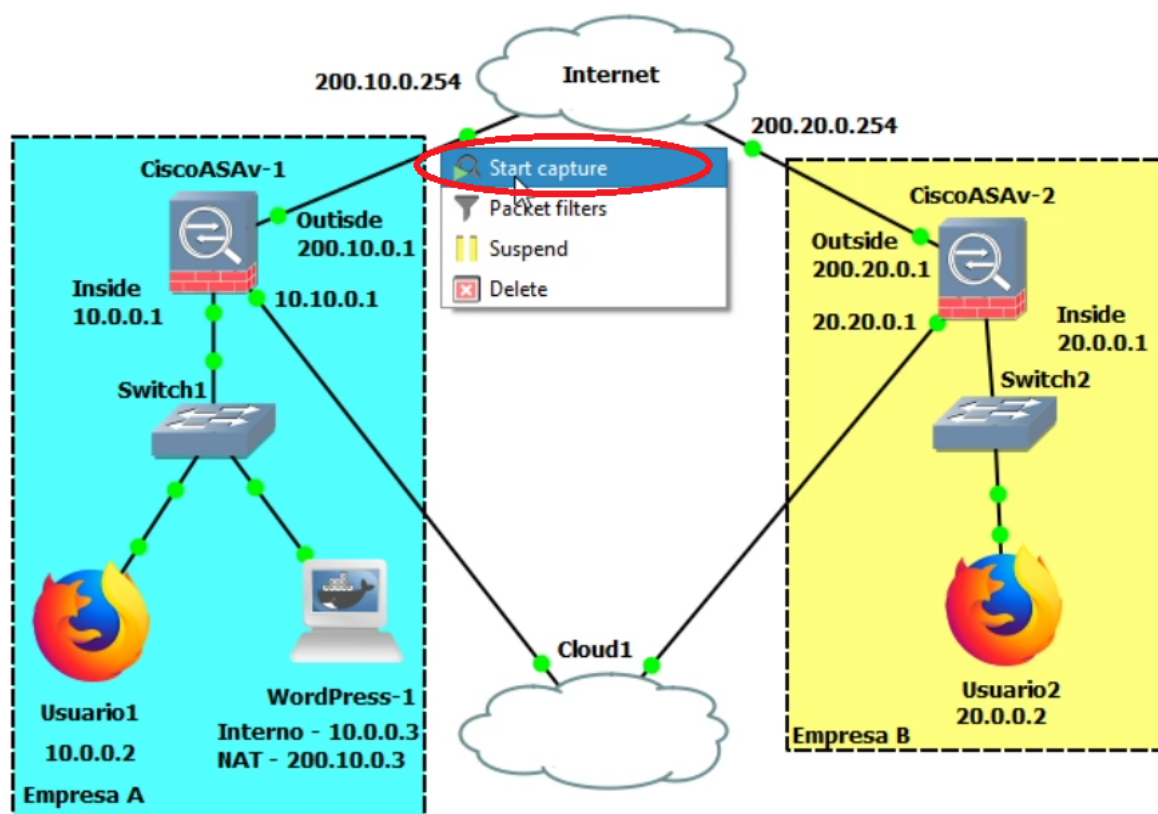


Preparando o ambiente

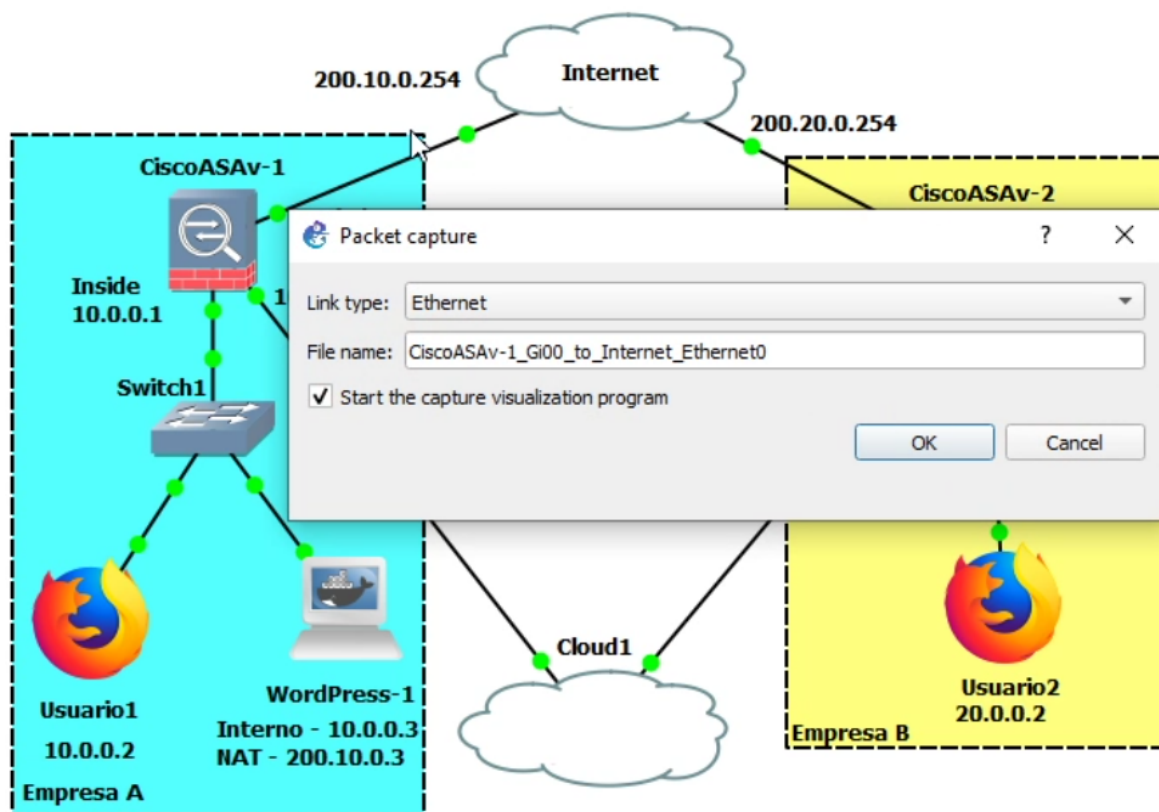
A ferramenta “Wireshark”, que já vem instalada em conjunto com o GNS3, é uma ferramenta de análise de dados extremamente poderosa.

Utilizamos ela para capturar e analisar os dados que estão trafegando da Empresa A para a Empresa B.

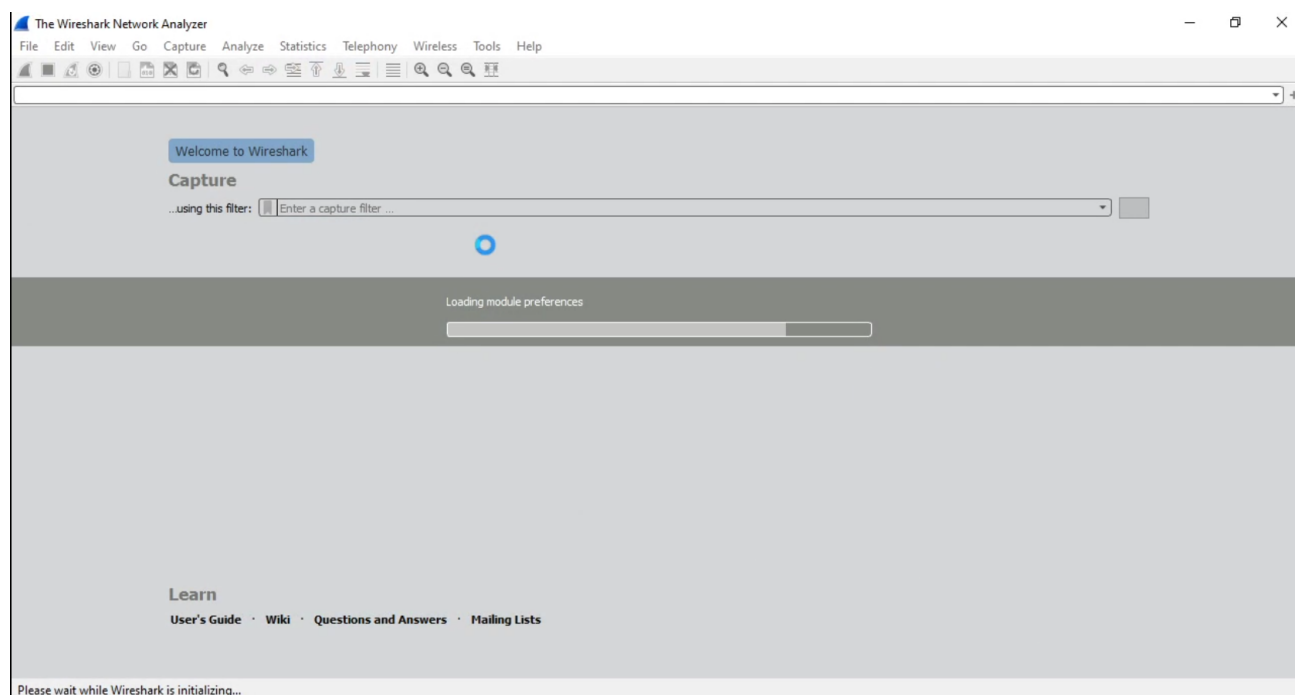
Para capturar os pacotes, basta clicar com o botão direito sobre o segmento de rede que se deseja analisar e então clicar em **Start capture**:



A seguir, é apresentada a janela para criação da captura, com as opções de tipo de link, nome do arquivo e inicializar a visualização em programa de captura:



Clicando em **OK**, o “Wireshark” será inicializado:



E então, basta gerar o tráfego que queremos analisar que os pacotes já serão capturados e apresentados dentro do “Wireshark”.

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. Packet 40, at time 19.772858, is an ESP packet from 200.10.0.1 to 200.20.0.1, with a length of 134 bytes. The bottom pane shows the details of this packet, identifying it as an Internet Security Association and Key Management Protocol (IPsec) packet. The packet structure is detailed in the packet bytes pane at the bottom, showing the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
37	19.758761	200.10.0.1	200.20.0.1	ESP	134	ESP (SPI=0x164b6fff6)
38	19.764387	200.20.0.1	200.10.0.1	ESP	134	ESP (SPI=0x3dbf8251)
39	19.764417	200.20.0.1	200.10.0.1	ESP	710	ESP (SPI=0x3dbf8251)
40	19.772858	200.10.0.1	200.20.0.1	ESP	134	ESP (SPI=0x164b6fff6)
41	19.800477	200.10.0.1	200.20.0.1	ESP	1494	ESP (SPI=0x164b6fff6)
42	19.804983	200.10.0.1	200.20.0.1	ESP	1094	ESP (SPI=0x164b6fff6)
43	19.814820	200.20.0.1	200.10.0.1	ESP	134	ESP (SPI=0x3dbf8251)
44	19.818139	200.20.0.1	200.10.0.1	ESP	134	ESP (SPI=0x3dbf8251)

Frame 1: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface -, id 0
> Ethernet II, Src: 0c:4d:c7:5b:3b:00 (0c:4d:c7:5b:3b:00), Dst: 0c:4d:c7:ff:6c:01 (0c:4d:c7:ff:6c:01)
> Internet Protocol Version 4, Src: 200.20.0.1, Dst: 200.10.0.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
> Internet Security Association and Key Management Protocol

0000 0c 4d c7 ff 6c 01 0c 4d c7 5b 3b 00 08 00 45 00 .M..l..M.[;...E.
0010 00 78 59 3f 00 00 fe 11 d3 14 c8 14 00 01 c8 0a .xY?.....
0020 00 01 01 f4 01 f4 00 64 c3 c5 3e fa e1 5f fe 98d->..._
0030 8c 7e c6 39 ae 8f 56 7c c8 47 00 10 05 01 a1 0a ~9..V|G.....
0040 ba 44 00 00 00 5c 3c dc 2a db d8 b9 58 65 39 e5 .D...<*...Xe9-
0050 84 ff af f1 e3 98 05 6d fd 59 24 36 08 0e 3c 51m-Y\$-<Q
0060 77 90 6e 5d 9c aa 5e bb 2c 43 95 69 e1 8f 31 6f win]..^..C i...lo
0070 3c be 90 23 03 36 26 63 8e 14 66 d0 06 03 0e aa <..#6&c..f.....
0080 03 40 1d f1 d1 3b @...;

Faça testes! Capture outros pacotes em outros segmentos dentro da rede e bons estudos!