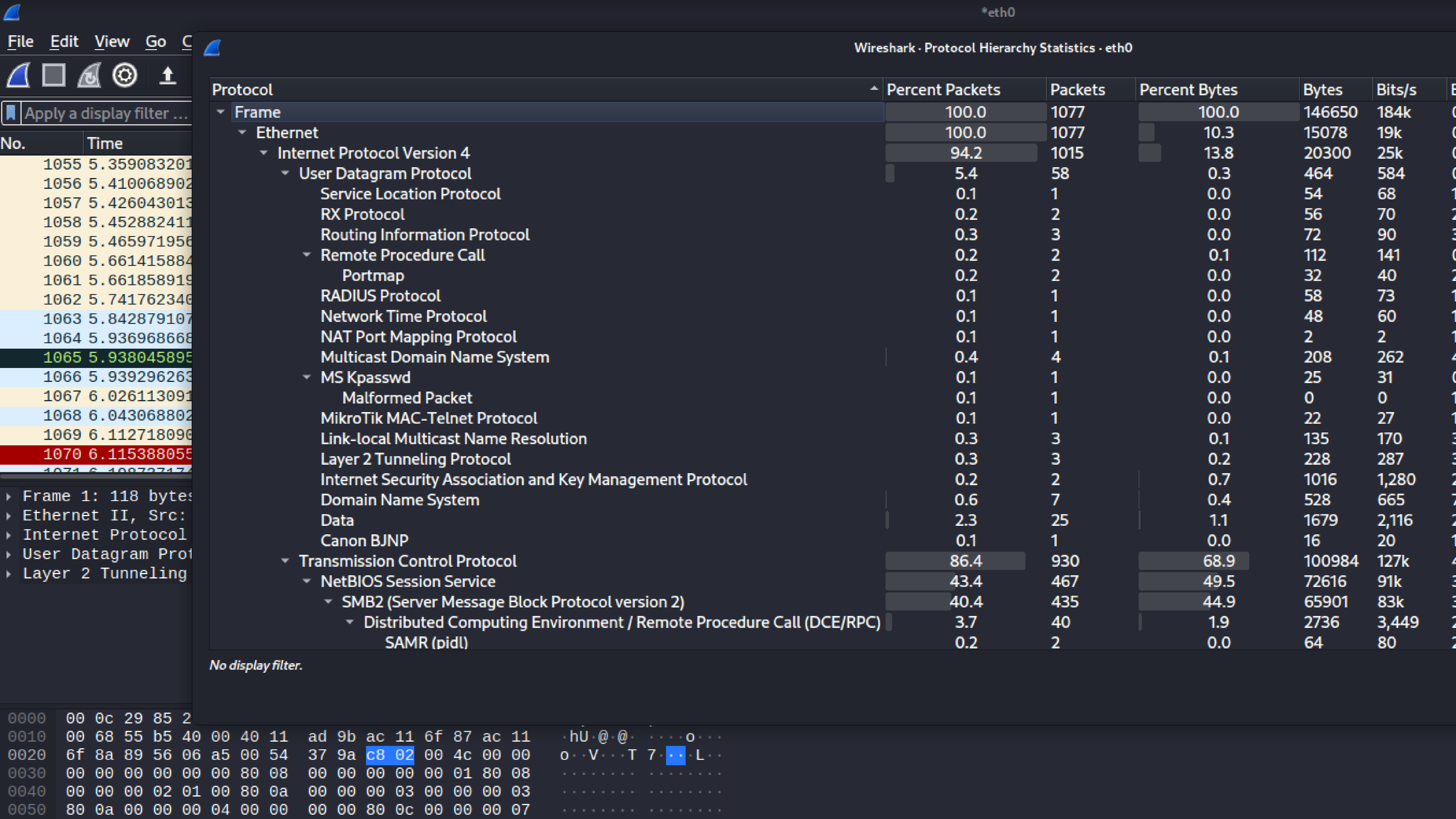
NETWORK/SERVER SECURITY



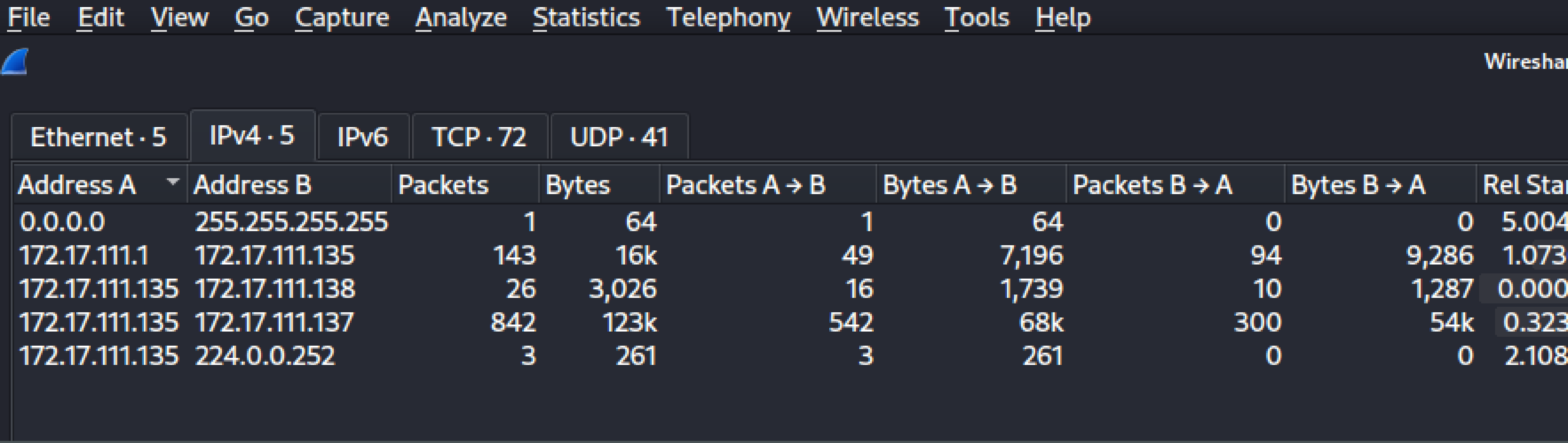
```
No.   Time
1055 5.359083201
1056 5.410068902
1057 5.426043013
1058 5.452882411
1059 5.465971956
1060 5.661415884
1061 5.661858919
1062 5.741762340
1063 5.842879107
1064 5.936968668
1065 5.938045895
1066 5.939296263
1067 6.026113091
1068 6.043068802
1069 6.112718090
1070 6.115388055
```

```
▸ Frame 1: 118 bytes
▸ Ethernet II, Src:
▸ Internet Protocol
▸ User Datagram Prot
▸ Layer 2 Tunneling
```

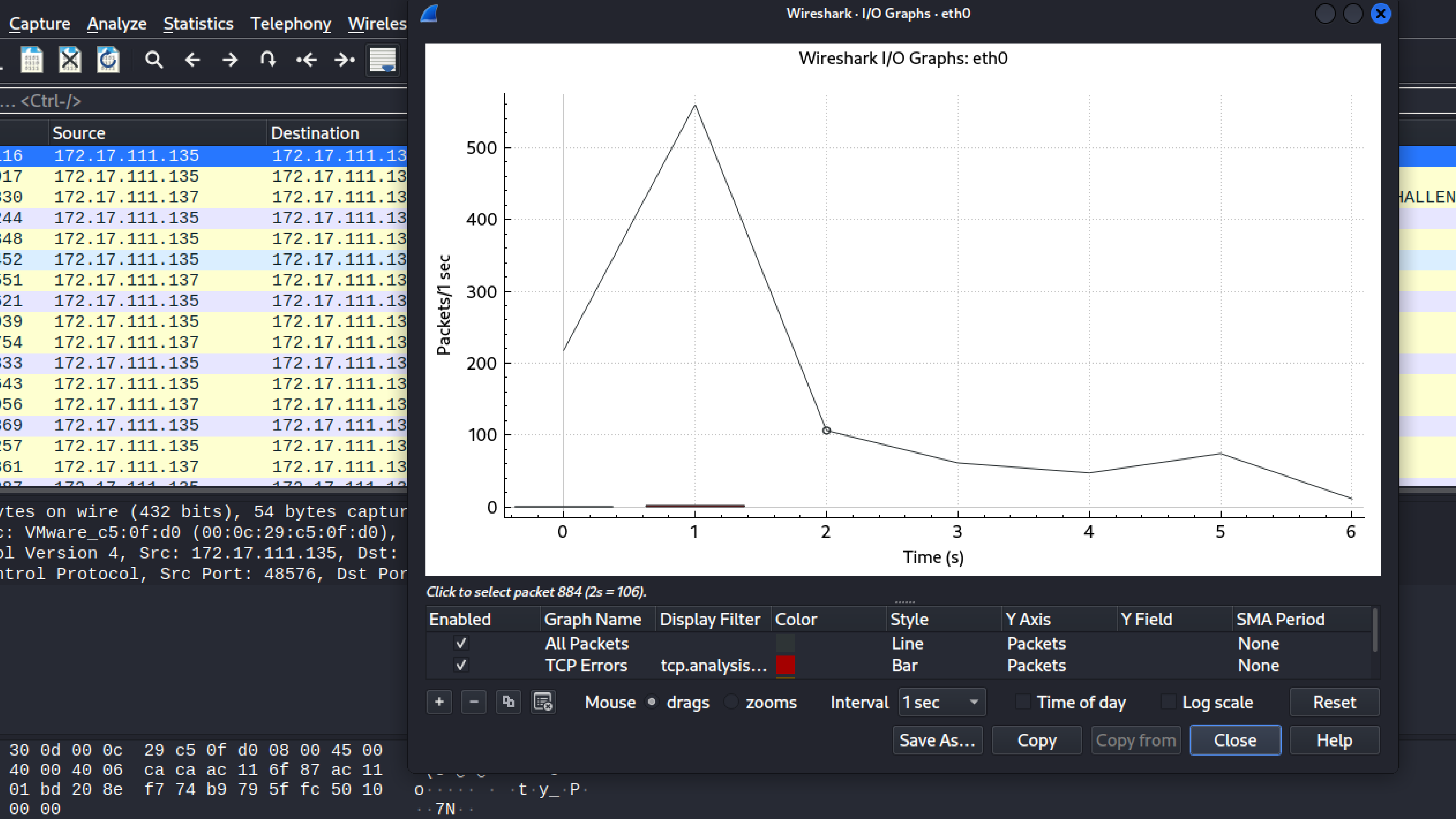
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	1077	100.0	146650	184k
Ethernet	100.0	1077	10.3	15078	19k
Internet Protocol Version 4	94.2	1015	13.8	20300	25k
User Datagram Protocol	5.4	58	0.3	464	584
Service Location Protocol	0.1	1	0.0	54	68
RX Protocol	0.2	2	0.0	56	70
Routing Information Protocol	0.3	3	0.0	72	90
Remote Procedure Call	0.2	2	0.1	112	141
Portmap	0.2	2	0.0	32	40
RADIUS Protocol	0.1	1	0.0	58	73
Network Time Protocol	0.1	1	0.0	48	60
NAT Port Mapping Protocol	0.1	1	0.0	2	2
Multicast Domain Name System	0.4	4	0.1	208	262
MS Kpasswd	0.1	1	0.0	25	31
Malformed Packet	0.1	1	0.0	0	0
MikroTik MAC-Telnet Protocol	0.1	1	0.0	22	27
Link-local Multicast Name Resolution	0.3	3	0.1	135	170
Layer 2 Tunneling Protocol	0.3	3	0.2	228	287
Internet Security Association and Key Management Protocol	0.2	2	0.7	1016	1,280
Domain Name System	0.6	7	0.4	528	665
Data	2.3	25	1.1	1679	2,116
Canon BJNP	0.1	1	0.0	16	20
Transmission Control Protocol	86.4	930	68.9	100984	127k
NetBIOS Session Service	43.4	467	49.5	72616	91k
SMB2 (Server Message Block Protocol version 2)	40.4	435	44.9	65901	83k
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	3.7	40	1.9	2736	3,449
SAMR (pidl)	0.2	2	0.0	64	80

No display filter.

```
0000  00 0c 29 85 2
0010  00 68 55 b5 40 00 40 11  ad 9b ac 11 6f 87 ac 11   ·hU·@·@· ····o···
0020  6f 8a 89 56 06 a5 00 54  37 9a c8 02 00 4c 00 00   o··V···T 7···L··
0030  00 00 00 00 00 00 80 08  00 00 00 00 00 01 80 08   ········ ········
0040  00 00 00 02 01 00 80 0a  00 00 00 03 00 00 00 03   ········ ········
0050  80 0a 00 00 00 04 00 00  00 00 80 0c 00 00 00 07   ········ ········
```



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Star
0.0.0.0	255.255.255.255	1	64	1	64	0	0	5.004
172.17.111.1	172.17.111.135	143	16k	49	7,196	94	9,286	1.073
172.17.111.135	172.17.111.138	26	3,026	16	1,739	10	1,287	0.000
172.17.111.135	172.17.111.137	842	123k	542	68k	300	54k	0.323
172.17.111.135	224.0.0.252	3	261	3	261	0	0	2.108



```
      Source            Destination
.16   172.17.111.135    172.17.111.13
017   172.17.111.135    172.17.111.13
330   172.17.111.137    172.17.111.13
244   172.17.111.135    172.17.111.13
348   172.17.111.135    172.17.111.13
152   172.17.111.135    172.17.111.13
551   172.17.111.137    172.17.111.13
521   172.17.111.135    172.17.111.13
039   172.17.111.135    172.17.111.13
754   172.17.111.137    172.17.111.13
333   172.17.111.135    172.17.111.13
543   172.17.111.135    172.17.111.13
056   172.17.111.137    172.17.111.13
369   172.17.111.135    172.17.111.13
257   172.17.111.135    172.17.111.13
361   172.17.111.137    172.17.111.13
```

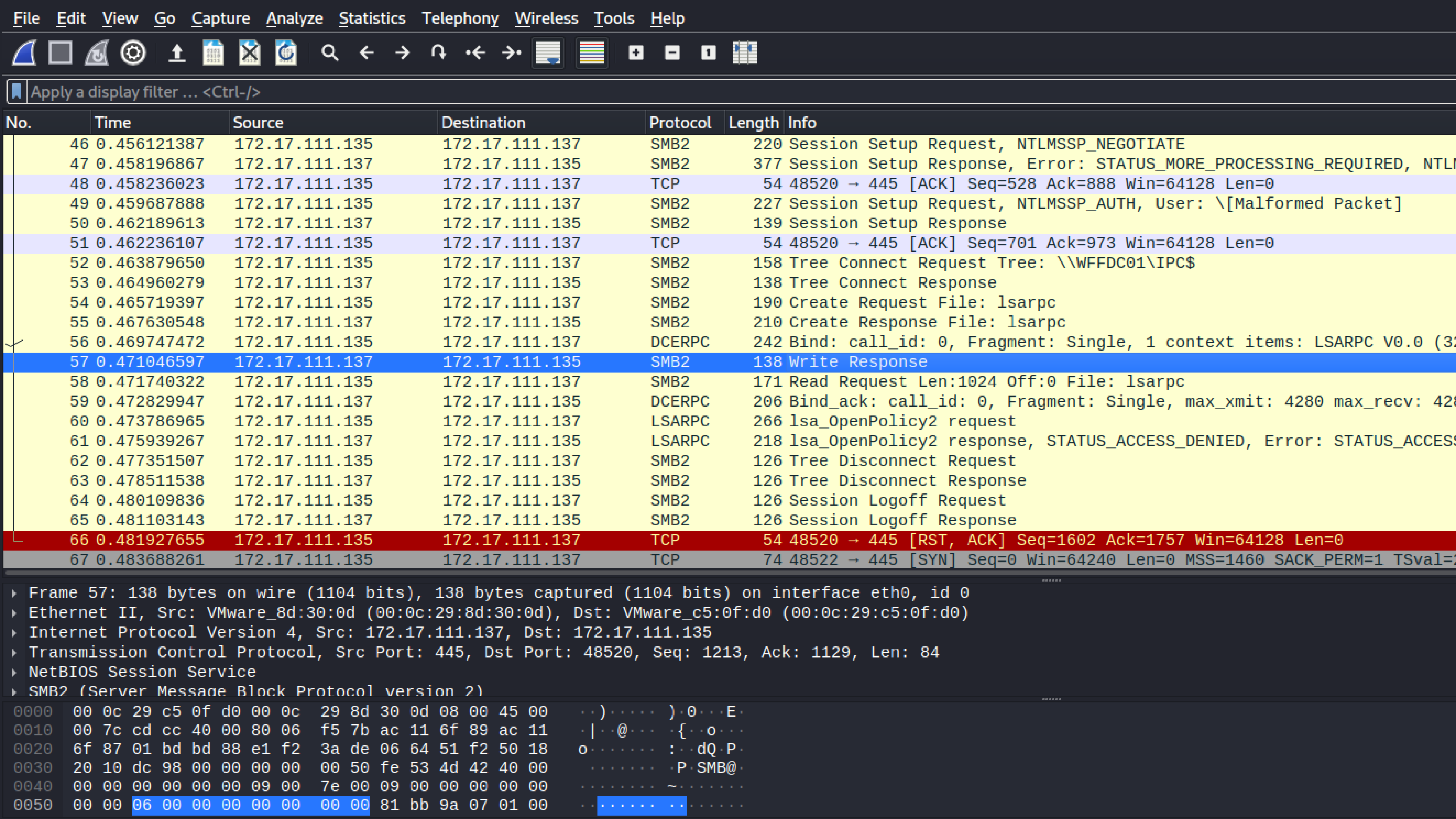
```
ytes on wire (432 bits), 54 bytes captur
c: VMware_c5:0f:d0 (00:0c:29:c5:0f:d0),
ol Version 4, Src: 172.17.111.135, Dst:
ntrol Protocol, Src Port: 48576, Dst Por
```

Click to select packet 884 (2s = 106).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
✓	All Packets		■	Line	Packets		None
✓	TCP Errors	tcp.analysis...	🟥	Bar	Packets		None

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale

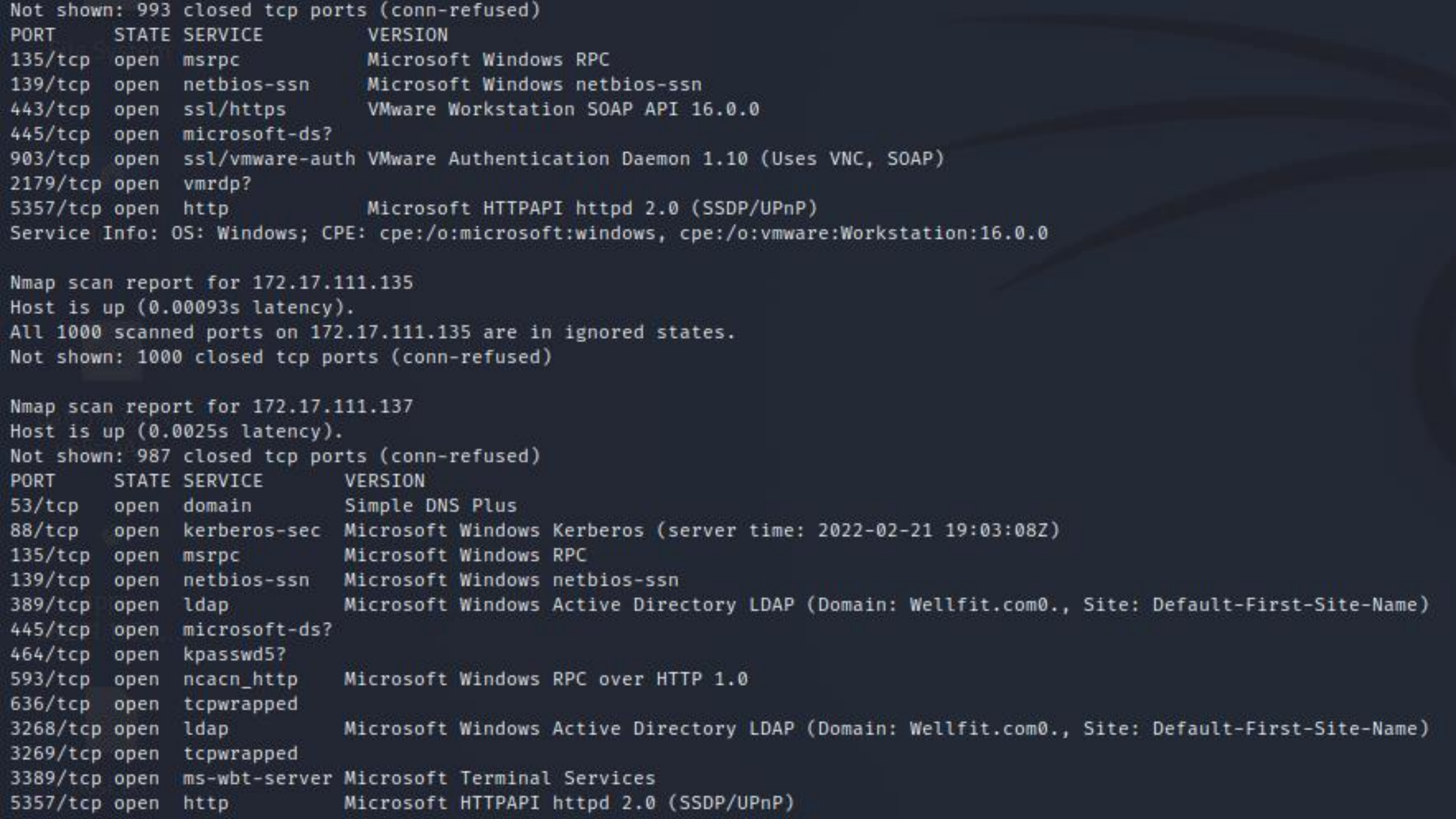
```
30 0d 00 0c  29 c5 0f d0 08 00 45 00
40 00 40 06  ca ca ac 11 6f 87 ac 11   
01 bd 20 8e  f7 74 b9 79 5f fc 50 10   o·····  ·t·y_·P·
00 00                                  ··7N··
```



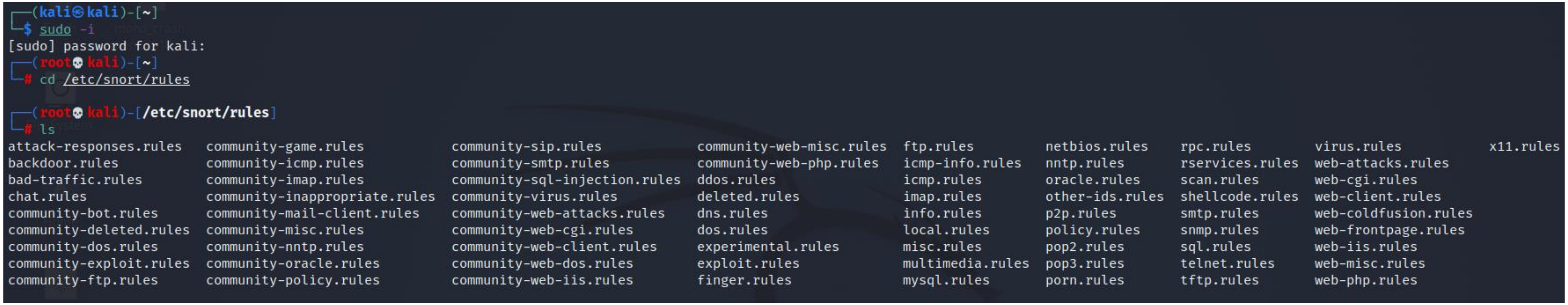
```
No.     Time         Source          Destination     Protocol  Length Info
     46 0.456121387  172.17.111.135  172.17.111.137  SMB2        220 Session Setup Request, NTLMSSP_NEGOTIATE
     47 0.458196867  172.17.111.137  172.17.111.135  SMB2        377 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLM
     48 0.458236023  172.17.111.135  172.17.111.137  TCP          54 48520 → 445 [ACK] Seq=528 Ack=888 Win=64128 Len=0
     49 0.459687888  172.17.111.135  172.17.111.137  SMB2        227 Session Setup Request, NTLMSSP_AUTH, User: \[Malformed Packet]
     50 0.462189613  172.17.111.137  172.17.111.135  SMB2        139 Session Setup Response
     51 0.462236107  172.17.111.135  172.17.111.137  TCP          54 48520 → 445 [ACK] Seq=701 Ack=973 Win=64128 Len=0
     52 0.463879650  172.17.111.135  172.17.111.137  SMB2        158 Tree Connect Request Tree: \\WFFDC01\IPC$
     53 0.464960279  172.17.111.137  172.17.111.135  SMB2        138 Tree Connect Response
     54 0.465719397  172.17.111.135  172.17.111.137  SMB2        190 Create Request File: lsarpc
     55 0.467630548  172.17.111.137  172.17.111.135  SMB2        210 Create Response File: lsarpc
     56 0.469747472  172.17.111.135  172.17.111.137  DCERPC      242 Bind: call_id: 0, Fragment: Single, 1 context items: LSARPC V0.0 (3
     57 0.471046597  172.17.111.137  172.17.111.135  SMB2        138 Write Response
     58 0.471740322  172.17.111.135  172.17.111.137  SMB2        171 Read Request Len:1024 Off:0 File: lsarpc
     59 0.472829947  172.17.111.137  172.17.111.135  DCERPC      206 Bind_ack: call_id: 0, Fragment: Single, max_xmit: 4280 max_recv: 42
     60 0.473786965  172.17.111.135  172.17.111.137  LSARPC      266 lsa_OpenPolicy2 request
     61 0.475939267  172.17.111.137  172.17.111.135  LSARPC      218 lsa_OpenPolicy2 response, STATUS_ACCESS_DENIED, Error: STATUS_ACCES
     62 0.477351507  172.17.111.135  172.17.111.137  SMB2        126 Tree Disconnect Request
     63 0.478511538  172.17.111.137  172.17.111.135  SMB2        126 Tree Disconnect Response
     64 0.480109836  172.17.111.135  172.17.111.137  SMB2        126 Session Logoff Request
     65 0.481103143  172.17.111.137  172.17.111.135  SMB2        126 Session Logoff Response
     66 0.481927655  172.17.111.135  172.17.111.137  TCP          54 48520 → 445 [RST, ACK] Seq=1602 Ack=1757 Win=64128 Len=0
     67 0.483688261  172.17.111.135  172.17.111.137  TCP          74 48522 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=
```

```
› Frame 57: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_8d:30:0d (00:0c:29:8d:30:0d), Dst: VMware_c5:0f:d0 (00:0c:29:c5:0f:d0)
› Internet Protocol Version 4, Src: 172.17.111.137, Dst: 172.17.111.135
› Transmission Control Protocol, Src Port: 445, Dst Port: 48520, Seq: 1213, Ack: 1129, Len: 84
› NetBIOS Session Service
› SMB2 (Server Message Block Protocol version 2)
```

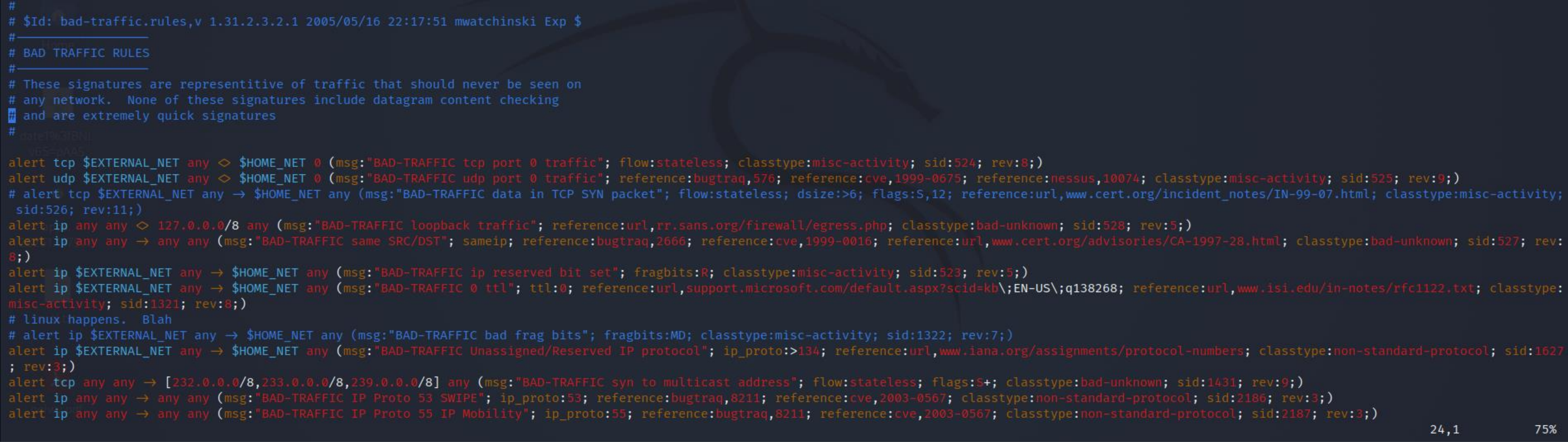
```
0000  00 0c 29 c5 0f d0 00 0c  29 8d 30 0d 08 00 45 00   ··)·····)·0···E·
0010  00 7c cd cc 40 00 80 06  f5 7b ac 11 6f 89 ac 11   ·|··@····{··o···
0020  6f 87 01 bd bd 88 e1 f2  3a de 06 64 51 f2 50 18   o·······:··dQ·P·
0030  20 10 dc 98 00 00 00 00  00 50 fe 53 4d 42 40 00    ·······P·SMB@·
0040  00 00 00 00 00 00 09 00  7e 00 09 00 00 00 00 00   ········~·······
0050  00 00 06 00 00 00 00 00  00 00 81 bb 9a 07 01 00   ················
```



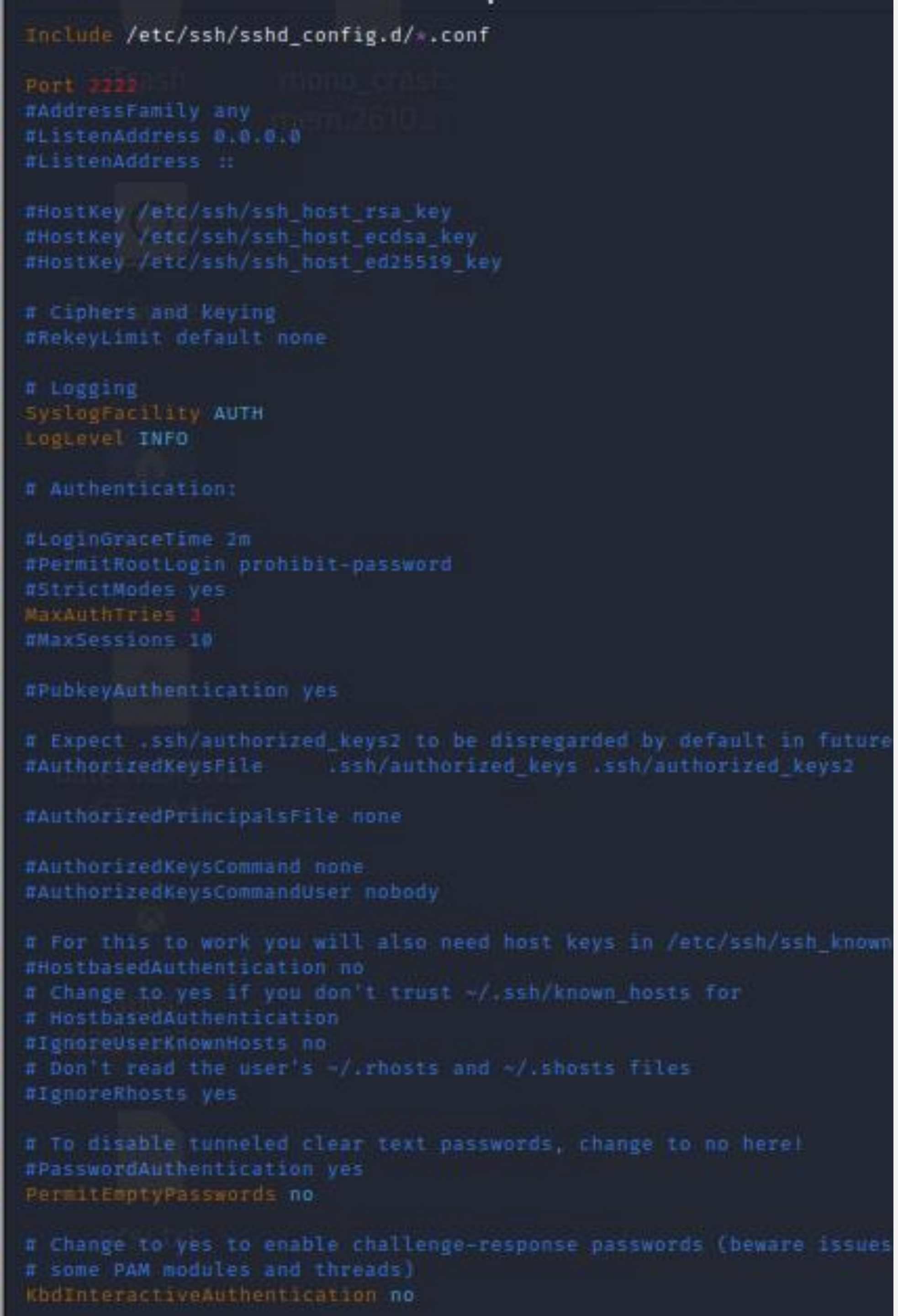
```
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp  open  ssl/https       VMware Workstation SOAP API 16.0.0
445/tcp  open  microsoft-ds?
903/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
2179/tcp open  vmrdp?
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:vmware:Workstation:16.0.0

Nmap scan report for 172.17.111.135
Host is up (0.00093s latency).
All 1000 scanned ports on 172.17.111.135 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 172.17.111.137
Host is up (0.0025s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-02-21 19:03:08Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: Wellfit.com0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: Wellfit.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```



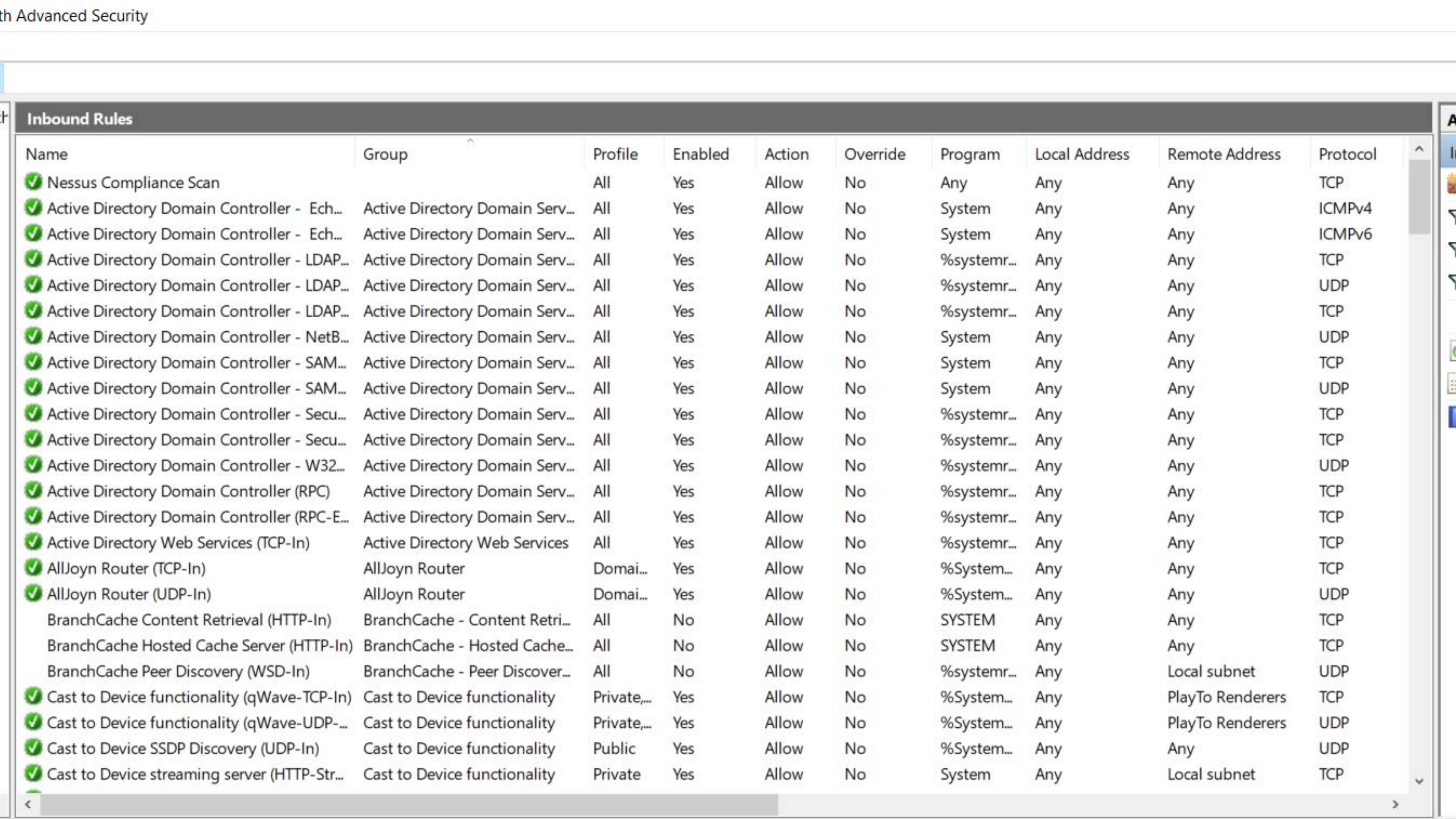
```
┌──(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root💀kali)-[~]
└─# cd /etc/snort/rules

┌──(root💀kali)-[/etc/snort/rules]
└─# ls
attack-responses.rules   community-game.rules           community-sip.rules            community-web-misc.rules  ftp.rules         netbios.rules    rpc.rules        virus.rules             x11.rules
backdoor.rules           community-icmp.rules           community-smtp.rules           community-web-php.rules   icmp-info.rules   nntp.rules       rservices.rules  web-attacks.rules
bad-traffic.rules        community-imap.rules           community-sql-injection.rules  ddos.rules                icmp.rules        oracle.rules     scan.rules       web-cgi.rules
chat.rules               community-inappropriate.rules  community-virus.rules          deleted.rules             imap.rules        other-ids.rules  shellcode.rules  web-client.rules
community-bot.rules      community-mail-client.rules    community-web-attacks.rules    dns.rules                 info.rules        p2p.rules        smtp.rules       web-coldfusion.rules
community-deleted.rules  community-misc.rules           community-web-cgi.rules        dos.rules                 local.rules       policy.rules     snmp.rules       web-frontpage.rules
community-dos.rules      community-nntp.rules           community-web-client.rules     experimental.rules        misc.rules        pop2.rules       sql.rules        web-iis.rules
community-exploit.rules  community-oracle.rules         community-web-dos.rules        exploit.rules             multimedia.rules  pop3.rules       telnet.rules     web-misc.rules
community-ftp.rules      community-policy.rules         community-web-iis.rules        finger.rules              mysql.rules       porn.rules       tftp.rules       web-php.rules
```



```
#
# $Id: bad-traffic.rules,v 1.31.2.3.2.1 2005/05/16 22:17:51 mwatchinski Exp $
#-----------------
# BAD TRAFFIC RULES
#-----------------
# These signatures are representitive of traffic that should never be seen on
# any network.  None of these signatures include datagram content checking
# and are extremely quick signatures
#

alert tcp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC tcp port 0 traffic"; flow:stateless; classtype:misc-activity; sid:524; rev:8;)
alert udp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC udp port 0 traffic"; reference:bugtraq,576; reference:cve,1999-0675; reference:nessus,10074; classtype:misc-activity; sid:525; rev:9;)
# alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC data in TCP SYN packet"; flow:stateless; dsize:>6; flags:S,12; reference:url,www.cert.org/incident_notes/IN-99-07.html; classtype:misc-activity;
 sid:526; rev:11;)
alert ip any any <> 127.0.0.0/8 any (msg:"BAD-TRAFFIC loopback traffic"; reference:url,rr.sans.org/firewall/egress.php; classtype:bad-unknown; sid:528; rev:5;)
alert ip any any -> any any (msg:"BAD-TRAFFIC same SRC/DST"; sameip; reference:bugtraq,2666; reference:cve,1999-0016; reference:url,www.cert.org/advisories/CA-1997-28.html; classtype:bad-unknown; sid:527; rev:
8;)
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC ip reserved bit set"; fragbits:R; classtype:misc-activity; sid:523; rev:5;)
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC 0 ttl"; ttl:0; reference:url,support.microsoft.com/default.aspx?scid=kb\;EN-US\;q138268; reference:url,www.isi.edu/in-notes/rfc1122.txt; classtype:
misc-activity; sid:1321; rev:8;)
# linux happens.  Blah
# alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC bad frag bits"; fragbits:MD; classtype:misc-activity; sid:1322; rev:7;)
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC Unassigned/Reserved IP protocol"; ip_proto:>134; reference:url,www.iana.org/assignments/protocol-numbers; classtype:non-standard-protocol; sid:1627
; rev:3;)
alert tcp any any -> [232.0.0.0/8,233.0.0.0/8,239.0.0.0/8] any (msg:"BAD-TRAFFIC syn to multicast address"; flow:stateless; flags:S+; classtype:bad-unknown; sid:1431; rev:9;)
alert ip any any -> any any (msg:"BAD-TRAFFIC IP Proto 53 SWIPE"; ip_proto:53; reference:bugtraq,8211; reference:cve,2003-0567; classtype:non-standard-protocol; sid:2186; rev:3;)
alert ip any any -> any any (msg:"BAD-TRAFFIC IP Proto 55 IP Mobility"; ip_proto:55; reference:bugtraq,8211; reference:cve,2003-0567; classtype:non-standard-protocol; sid:2187; rev:3;)
                                                                                                                                                                                            24,1          75%
```



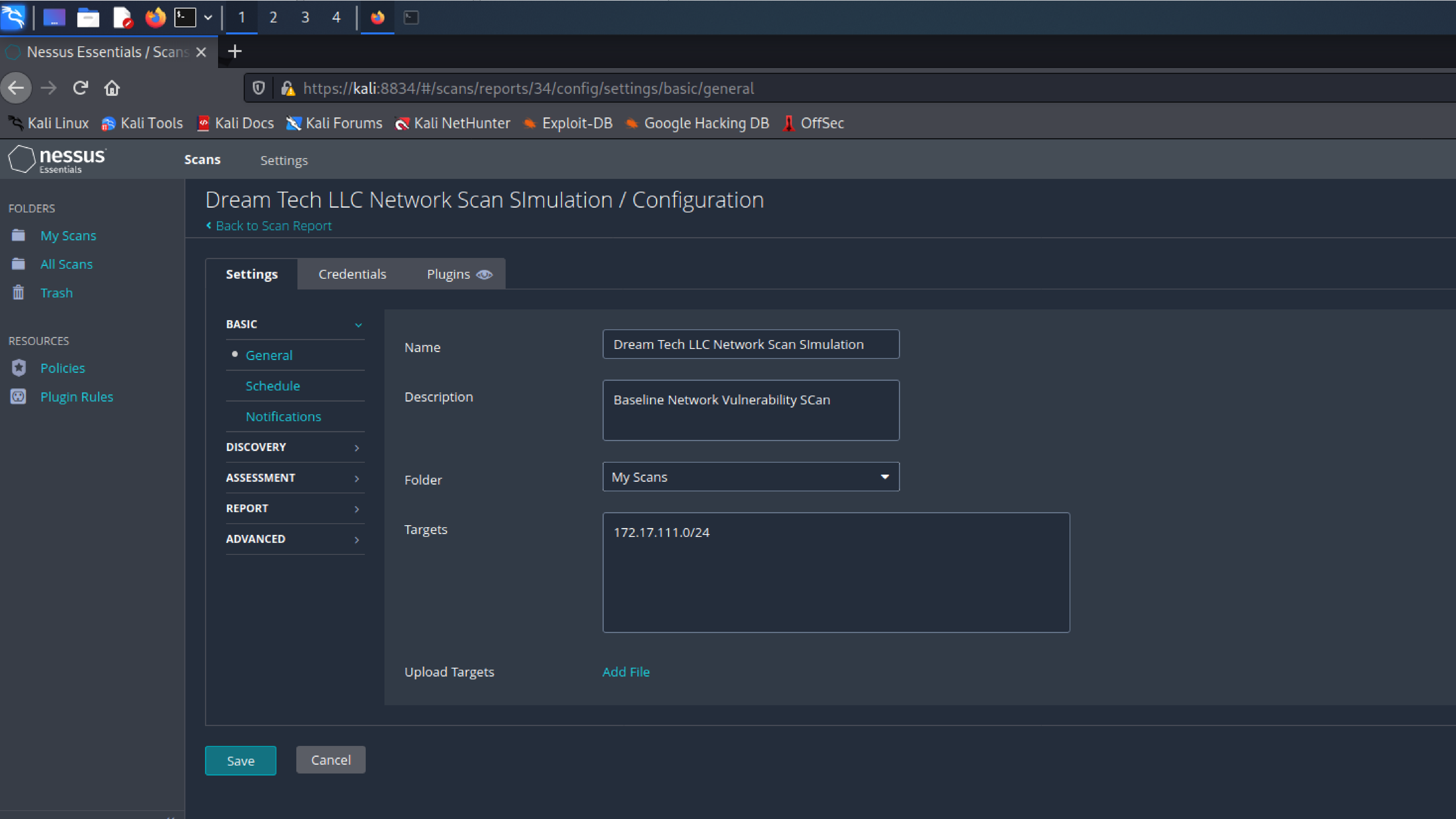
```
Include /etc/ssh/sshd_config.d/*.conf

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues
# some PAM modules and threads)
KbdInteractiveAuthentication no
```



th Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
✓ Nessus Compliance Scan		All	Yes	Allow	No	Any	Any	Any	TCP
✓ Active Directory Domain Controller - Ech...	Active Directory Domain Serv...	All	Yes	Allow	No	System	Any	Any	ICMPv4
✓ Active Directory Domain Controller - Ech...	Active Directory Domain Serv...	All	Yes	Allow	No	System	Any	Any	ICMPv6
✓ Active Directory Domain Controller - LDAP...	Active Directory Domain Serv...	All	Yes	Allow	No	%systemr...	Any	Any	TCP
✓ Active Directory Domain Controller - LDAP...	Active Directory Domain Serv...	All	Yes	Allow	No	%systemr...	Any	Any	UDP
✓ Active Directory Domain Controller - LDAP...	Active Directory Domain Serv...	All	Yes	Allow	No	%systemr...	Any	Any	TCP
✓ Active Directory Domain Controller - NetB...	Active Directory Domain Serv...	All	Yes	Allow	No	System	Any	Any	UDP
✓ Active Directory Domain Controller - SAM...	Active Directory Domain Serv...	All	Yes	Allow	No	System	Any	Any	TCP
✓ Active Directory Domain Controller - SAM...	Active Directory Domain Serv...	All	Yes	Allow	No	System	Any	Any	UDP
✓ Active Directory Domain Controller - Secu...	Active Directory Domain Serv...	All	Yes	Allow	No	%systemr...	Any	Any	TCP
✓ Active Directory Domain Controller - Secu...	Active Directory Domain Serv...	All	Yes	Allow	No	%systemr...	Any	Any	TCP
✓ Active Directory Domain Controller - W32...	Active Directory Domain Serv...	All	Yes	Allow	No	%systemr...	Any	Any	UDP
✓ Active Directory Domain Controller (RPC)	Active Directory Domain Serv...	All	Yes	Allow	No	%systemr...	Any	Any	TCP
✓ Active Directory Domain Controller (RPC-E...	Active Directory Domain Serv...	All	Yes	Allow	No	%systemr...	Any	Any	TCP
✓ Active Directory Web Services (TCP-In)	Active Directory Web Services	All	Yes	Allow	No	%systemr...	Any	Any	TCP
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retri...	All	No	Allow	No	SYSTEM	Any	Any	TCP
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache...	All	No	Allow	No	SYSTEM	Any	Any	TCP
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discover...	All	No	Allow	No	%systemr...	Any	Local subnet	UDP
✓ Cast to Device functionality (qWave-TCP-In)	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
✓ Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
✓ Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any	UDP
✓ Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local subnet	TCP



https://kali:8834/#/scans/reports/34/config/settings/basic/general

Dream Tech LLC Network Scan SImulation / Configuration

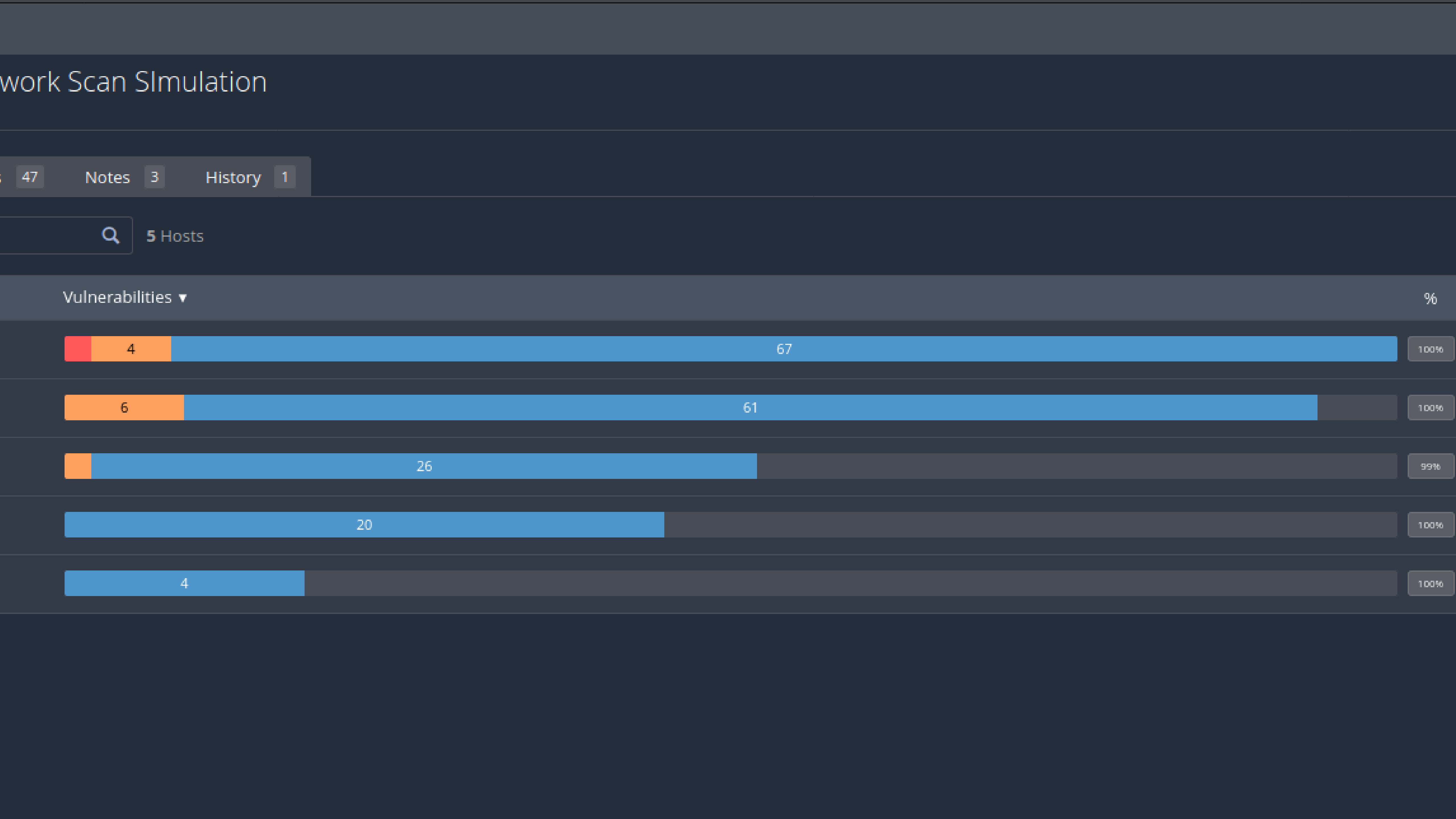
‹ Back to Scan Report

Name: Dream Tech LLC Network Scan SImulation

Description: Baseline Network Vulnerability SCan

Folder: My Scans

Targets: 172.17.111.0/24

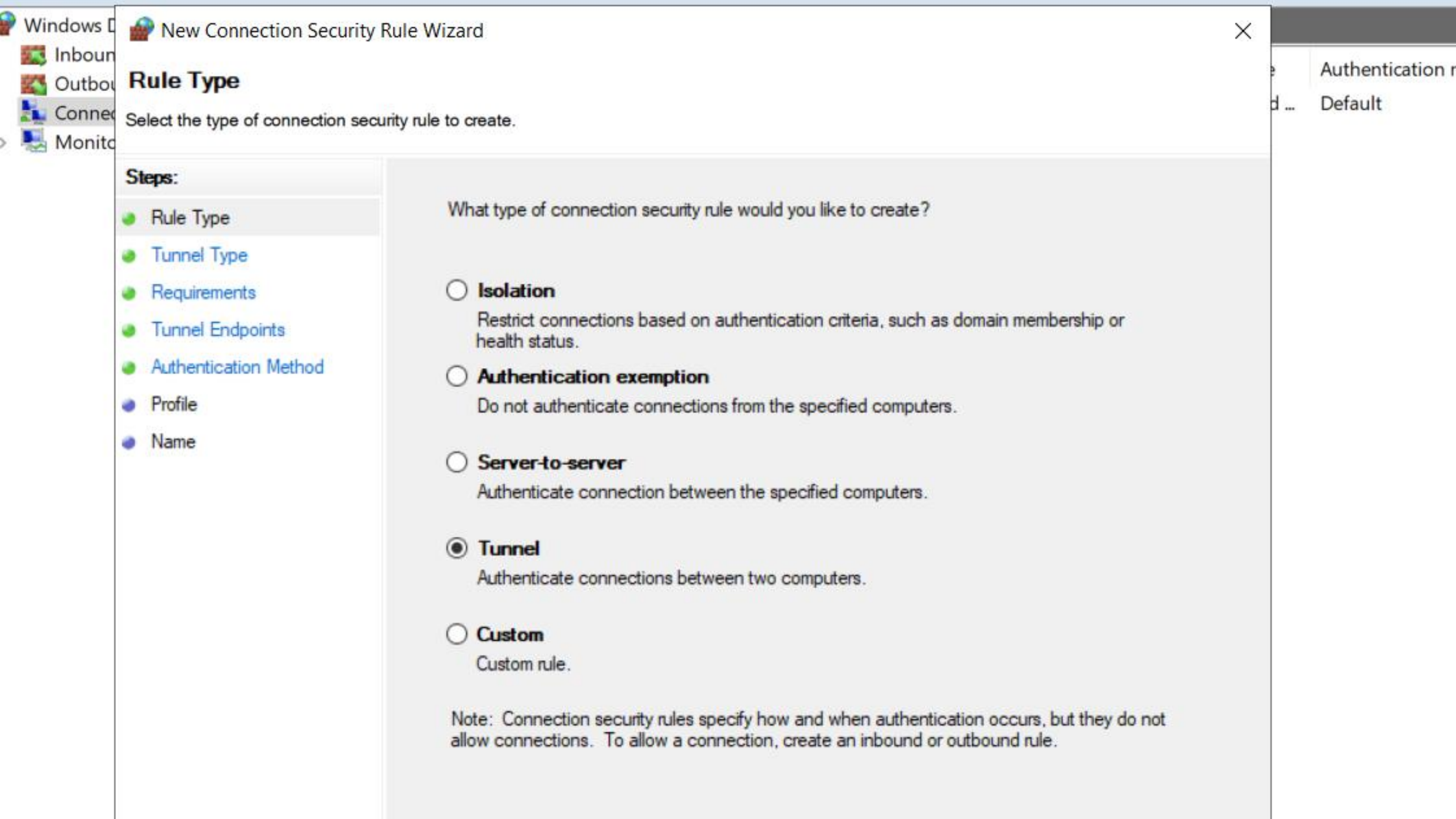


work Scan SImulation

s 47 Notes 3 History 1

5 Hosts

Vulnerabilities ▾	%
4 67	100%
6 61	100%
26	99%
20	100%
4	100%



New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Tunnel Type
- Requirements
- Tunnel Endpoints
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

○ **Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.

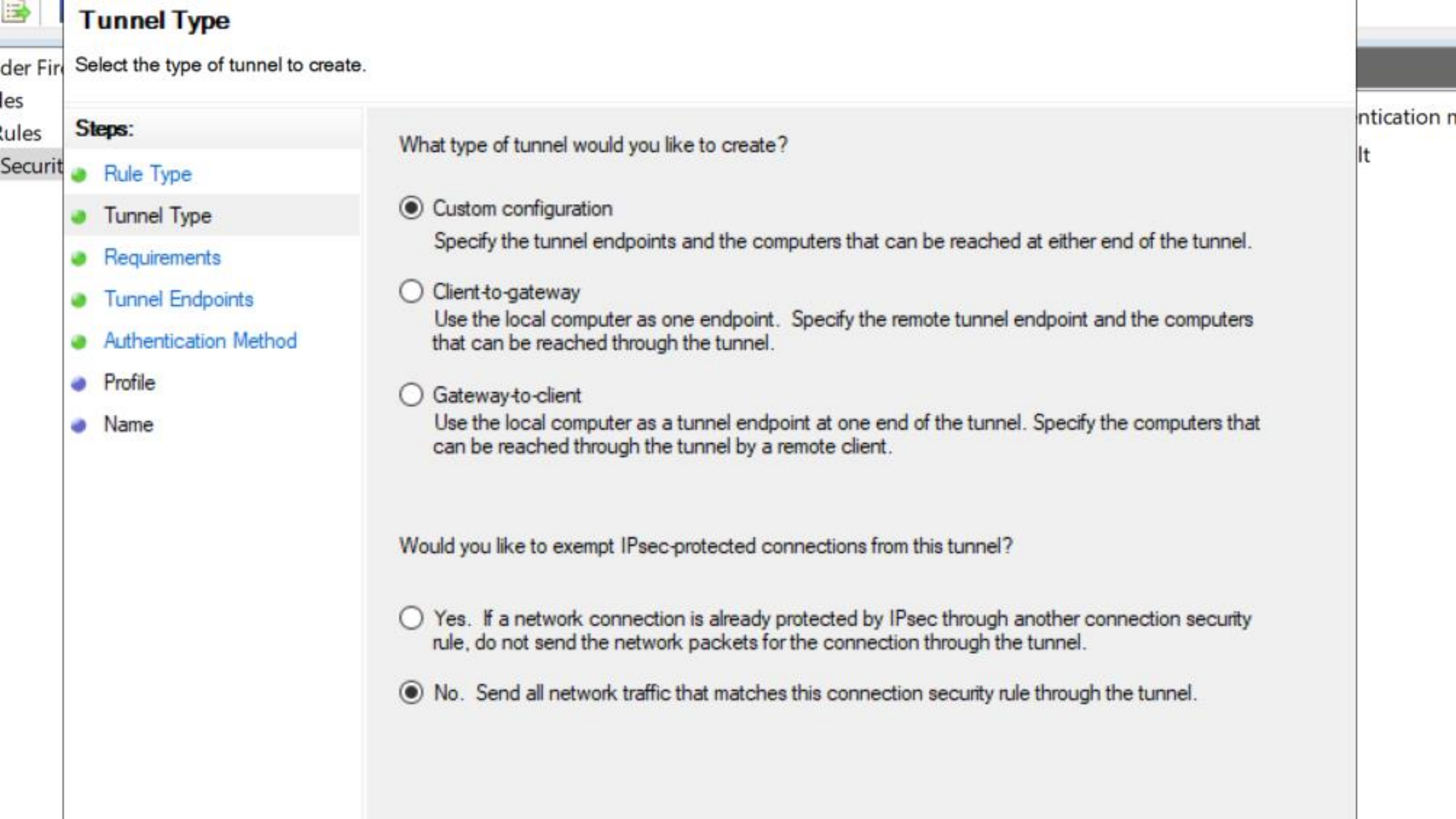
○ **Authentication exemption**
Do not authenticate connections from the specified computers.

○ **Server-to-server**
Authenticate connection between the specified computers.

● **Tunnel**
Authenticate connections between two computers.

○ **Custom**
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.



Tunnel Type

Select the type of tunnel to create.

Steps:

- Rule Type
- Tunnel Type
- Requirements
- Tunnel Endpoints
- Authentication Method
- Profile
- Name

What type of tunnel would you like to create?

● Custom configuration
Specify the tunnel endpoints and the computers that can be reached at either end of the tunnel.

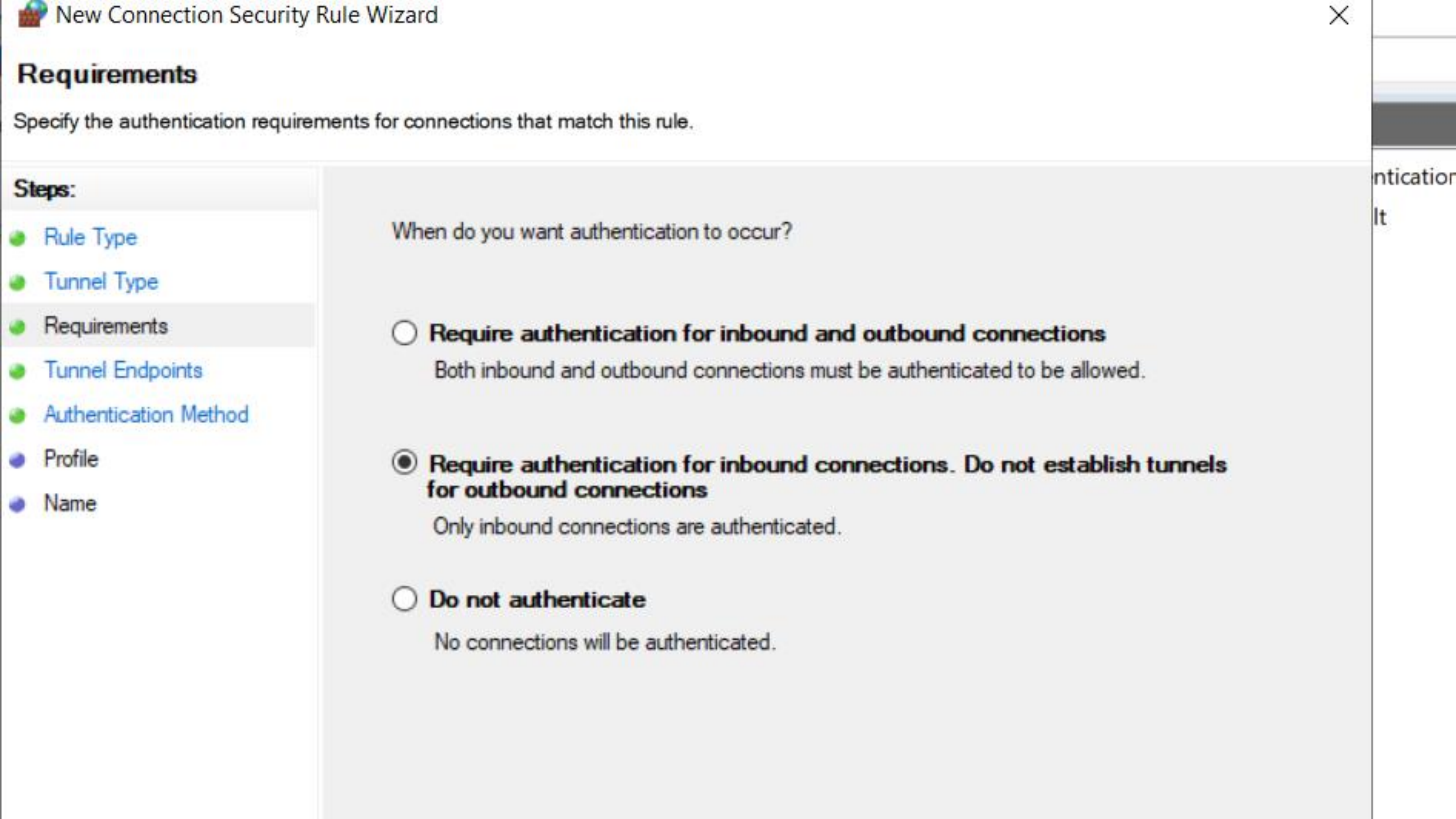
○ Client-to-gateway
Use the local computer as one endpoint. Specify the remote tunnel endpoint and the computers that can be reached through the tunnel.

○ Gateway-to-client
Use the local computer as a tunnel endpoint at one end of the tunnel. Specify the computers that can be reached through the tunnel by a remote client.

Would you like to exempt IPsec-protected connections from this tunnel?

○ Yes. If a network connection is already protected by IPsec through another connection security rule, do not send the network packets for the connection through the tunnel.

● No. Send all network traffic that matches this connection security rule through the tunnel.



New Connection Security Rule Wizard

Requirements

Specify the authentication requirements for connections that match this rule.

Steps:

- Rule Type
- Tunnel Type
- Requirements
- Tunnel Endpoints
- Authentication Method
- Profile
- Name

When do you want authentication to occur?

○ **Require authentication for inbound and outbound connections**

Both inbound and outbound connections must be authenticated to be allowed.

● **Require authentication for inbound connections. Do not establish tunnels for outbound connections**

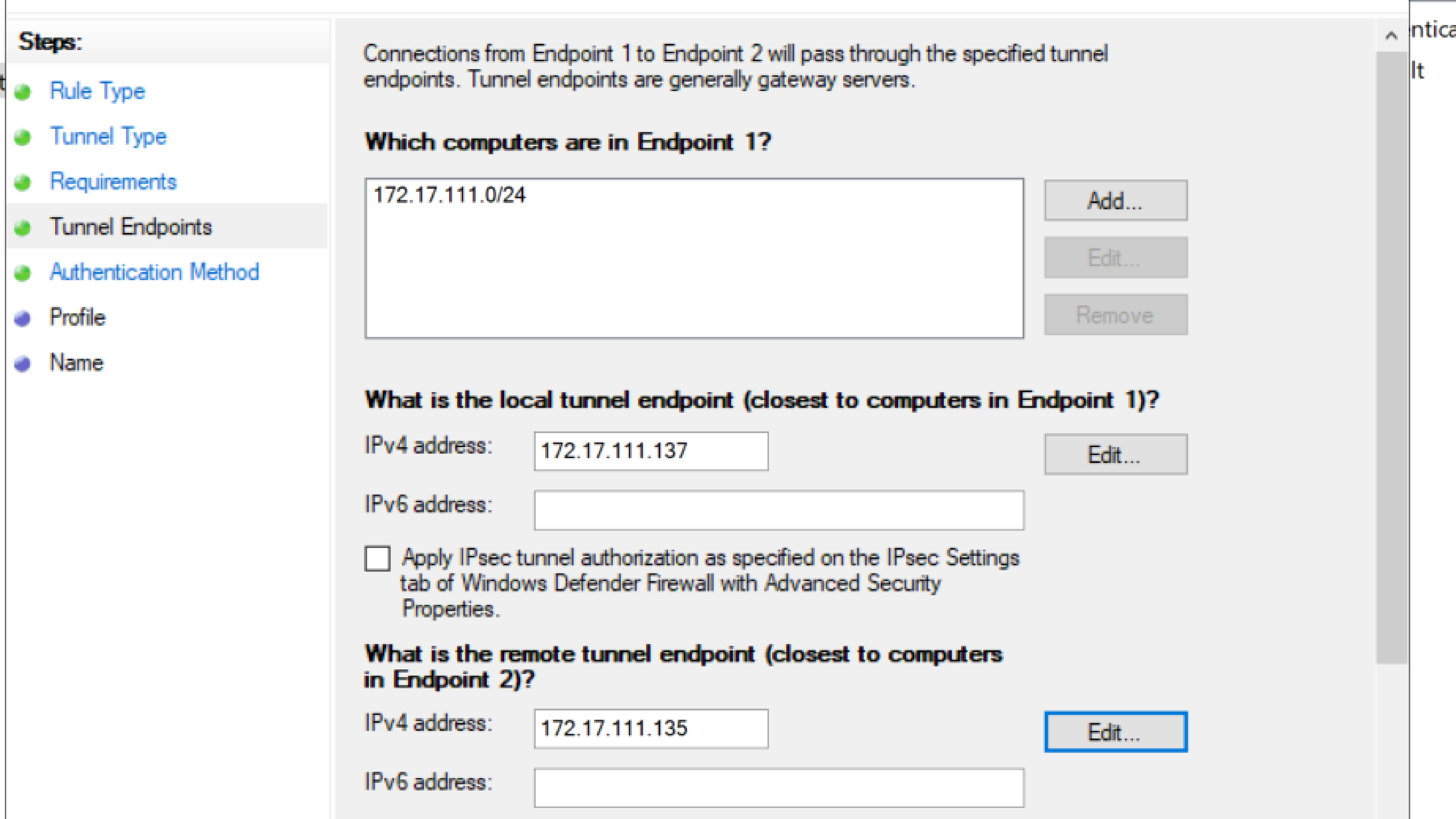
Only inbound connections are authenticated.

○ **Do not authenticate**

No connections will be authenticated.

ntication

lt



Connections from Endpoint 1 to Endpoint 2 will pass through the specified tunnel endpoints. Tunnel endpoints are generally gateway servers.

Which computers are in Endpoint 1?

172.17.111.0/24

What is the local tunnel endpoint (closest to computers in Endpoint 1)?

IPv4 address: 172.17.111.137

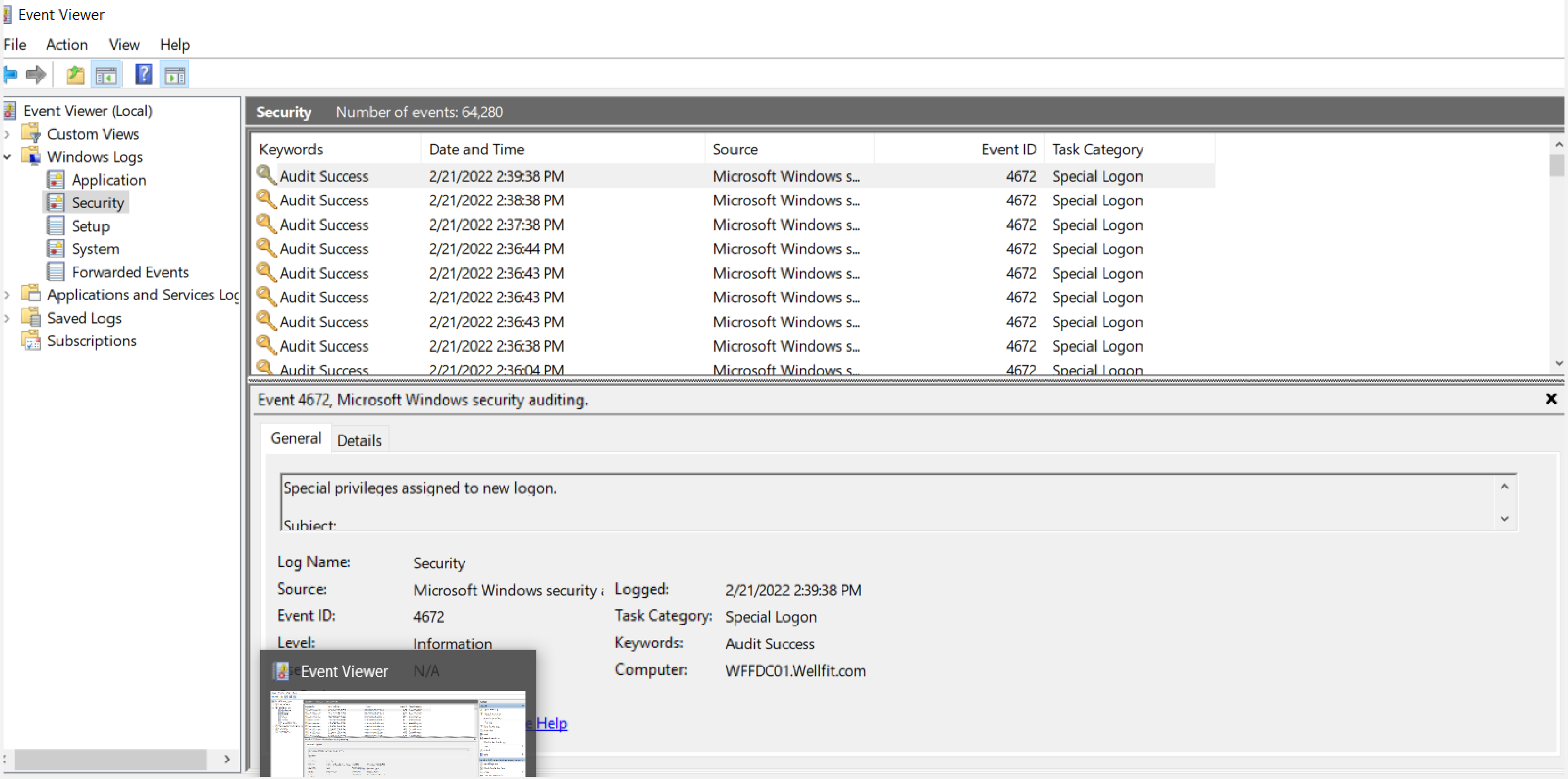
IPv6 address:

□ Apply IPsec tunnel authorization as specified on the IPsec Settings tab of Windows Defender Firewall with Advanced Security Properties.

What is the remote tunnel endpoint (closest to computers in Endpoint 2)?

IPv4 address: 172.17.111.135

IPv6 address:



Security Number of events: 64,280

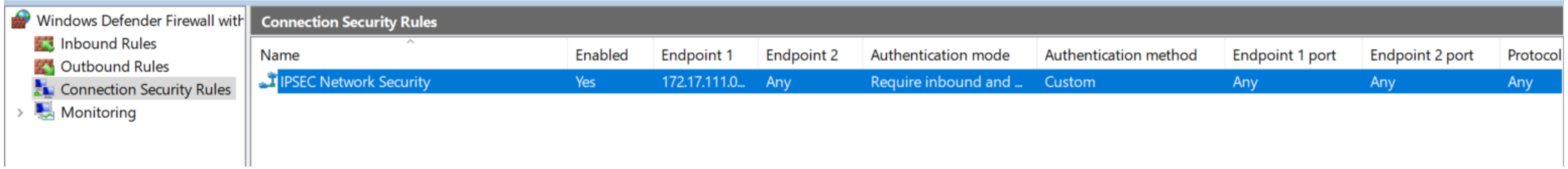
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/21/2022 2:39:38 PM	Microsoft Windows s...	4672	Special Logon
Audit Success	2/21/2022 2:38:38 PM	Microsoft Windows s...	4672	Special Logon
Audit Success	2/21/2022 2:37:38 PM	Microsoft Windows s...	4672	Special Logon
Audit Success	2/21/2022 2:36:44 PM	Microsoft Windows s...	4672	Special Logon
Audit Success	2/21/2022 2:36:43 PM	Microsoft Windows s...	4672	Special Logon
Audit Success	2/21/2022 2:36:43 PM	Microsoft Windows s...	4672	Special Logon
Audit Success	2/21/2022 2:36:43 PM	Microsoft Windows s...	4672	Special Logon
Audit Success	2/21/2022 2:36:38 PM	Microsoft Windows s...	4672	Special Logon
Audit Success	2/21/2022 2:36:04 PM	Microsoft Windows s...	4672	Special Logon

Event 4672, Microsoft Windows security auditing.

Special privileges assigned to new logon.

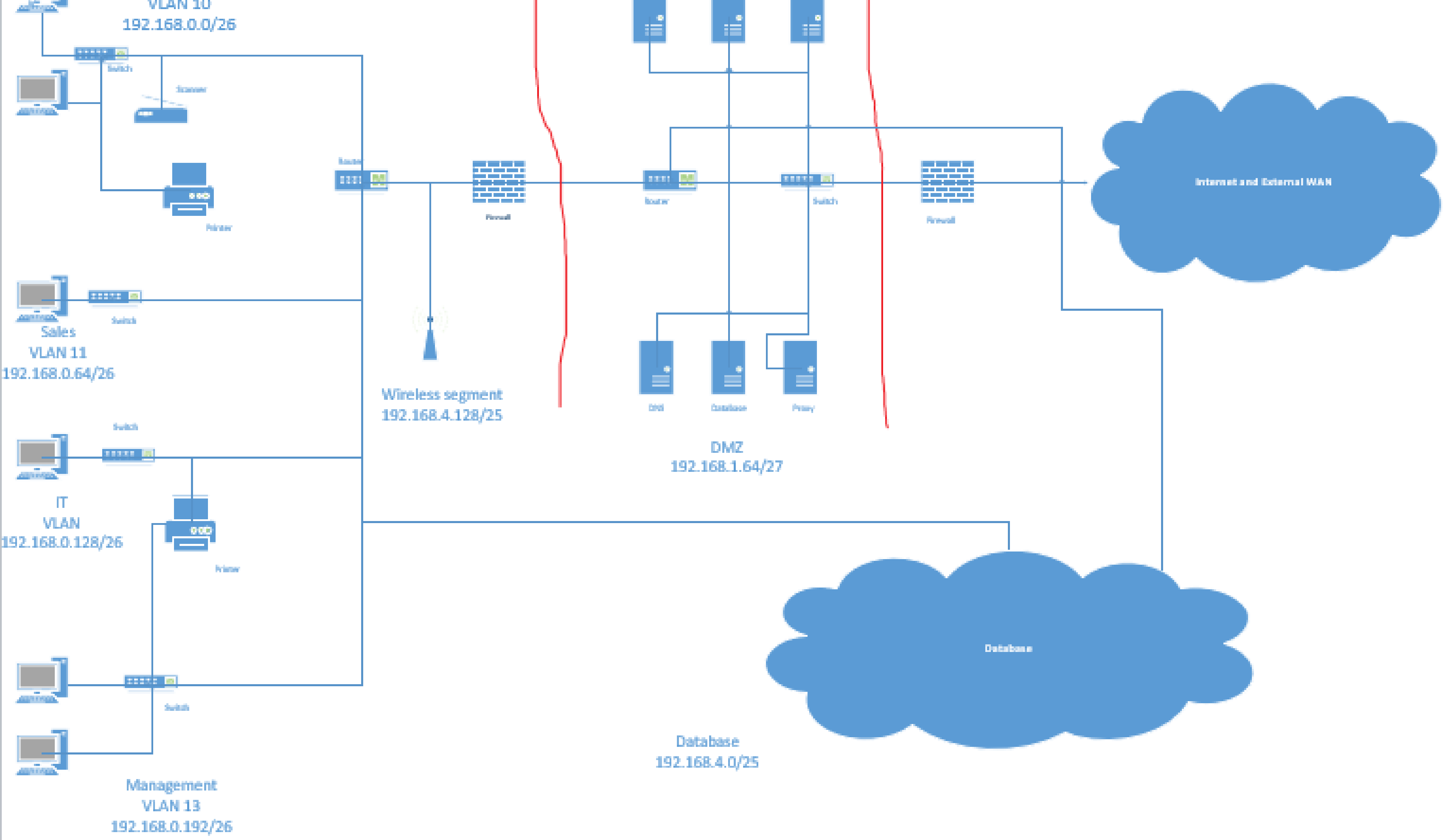
Subject:

Log Name: Security
Source: Microsoft Windows security a
Logged: 2/21/2022 2:39:38 PM
Event ID: 4672
Task Category: Special Logon
Level: Information
Keywords: Audit Success
N/A
Computer: WFFDC01.Wellfit.com



Connection Security Rules

Name	Enabled	Endpoint 1	Endpoint 2	Authentication mode	Authentication method	Endpoint 1 port	Endpoint 2 port	Protocol
IPSEC Network Security	Yes	172.17.111.0...	Any	Require inbound and ...	Custom	Any	Any	Any


VLAN 10
192.168.0.0/26
Switch
Scanner
Printer
Router
Firewall
Router
Switch
Firewall
Internet and External WAN
Sales
VLAN 11
192.168.0.64/26
Switch
Wireless segment
192.168.4.128/25
DNS
Database
Proxy
DMZ
192.168.1.64/27
Switch
IT
VLAN
192.168.0.128/26
Printer
Database
Switch
Database
192.168.4.0/25
Management
VLAN 13
192.168.0.192/26