Filtros de Netflow en PRTG

Filtros de Netflow para PRTG

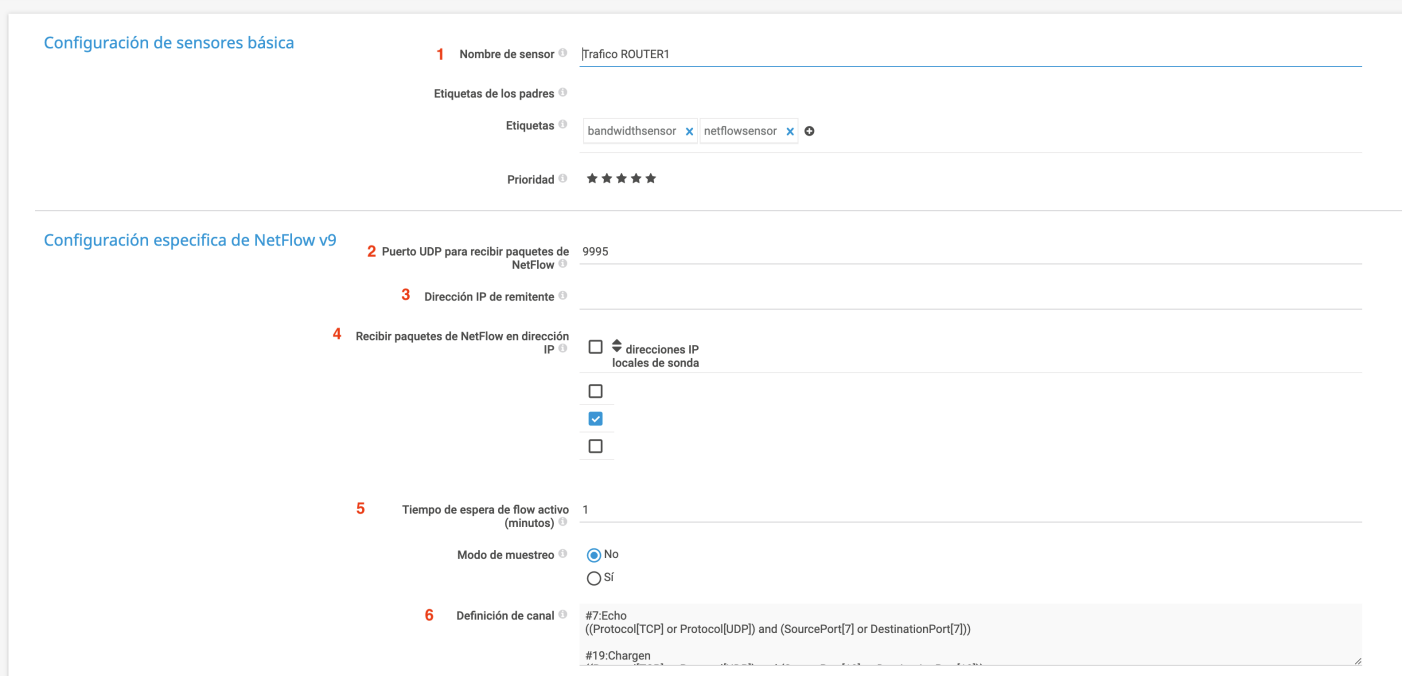
El protocolo NetFlow está soportado principalmente por routers y switches Cisco.

NetFlow permite analizar y monitorizar el ancho de banda y determinar, por ejemplo, la cantidad de tráfico causado por las direcciones IP, protocolos o programas.

Para llevar a cabo dicho análisis, se configuran los routers o switches de tal manera que los paquetes de flujo son enviados a un ordenador que tenga instalada una sonda PRTG. La tecnología de flujo supone poca carga de CPU y está especialmente adaptada para las redes con tráfico de datos pesados.

En este ejemplo se ve como puede segmentar el tráfico en función del tipo de protocolo (TCP, UDP, etc). El puerto origen. destino, o ambos.

Para crear un filtro Netflow, en primer lugar crearemos el sensor Netflow en nuestro servidor PRTG



partado 1

Escribiremos un nombre descriptivo

Apartado 2

El puerto UDP de PRTG que escuchará el tráfico que viene de nuestro equipo

Hay que comprobar que el puerto está abierto en el firewall de Windows

Apartado 3 (opcional)

Dirección IP del equipo que envía los datos

Apartado 4

Dirección IP del servidor PRTG que “escuchará”

Apartado 5

Timeout de las tramas Netflow

Apartado 6

Protocolos y su desglose, como podemos ver en el siguiente ejemplo

```
#7: Echo
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[7] or DestinationPort[7]))

#19: Chargen
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[19] or DestinationPort[19]))

#20: FTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[20] or DestinationPort[20]))

#21: FTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[21] or DestinationPort[21]))

#22: SSHSCP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[22] or DestinationPort[22]))

#23: Telnet
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[23] or DestinationPort[23]))

#25: SMTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[25] or DestinationPort[25]))

#42: WINSReplication
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[42] or DestinationPort[42]))

#43: WHOIS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[43] or DestinationPort[43]))

#49: TACACS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[49] or DestinationPort[49]))

#53: DNS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[53] or DestinationPort[53]))

#67: DHCPBOOTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[67] or DestinationPort[67]))
```

```
#68: DHCPBOOTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[68] or DestinationPort[68]))

#69: TFTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[69] or DestinationPort[69]))

#70: Gopher
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[70] or DestinationPort[70]))

#79: Finger
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[79] or DestinationPort[79]))

#80: HTTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[80] or DestinationPort[80]))

#88: Kerberos
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[88] or DestinationPort[88]))

#102: MSExchange
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[102] or DestinationPort[102]))

#110: POP3
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[110] or DestinationPort[110]))

#113: Ident
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[113] or DestinationPort[113]))

#119: NNTPUsenet
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[119] or DestinationPort[119]))

#123: NTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[123] or DestinationPort[123]))

#135: MicrosoftRPC
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[135] or DestinationPort[135]))

#137: NetBIOS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[137] or DestinationPort[137]))

#139: NetBIOS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[139] or DestinationPort[139]))

#143: IMAP4
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[143] or DestinationPort[143]))

#161: SNMP
((Protocol[UDP] or Protocol[UDP]) and (SourcePort[161] or DestinationPort[161]))

#162: SNMP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[162] or DestinationPort[162]))

#177: XDMCP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[177] or DestinationPort[177]))
```

```
#179: BGP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[179] or DestinationPort[179]))

#201: AppleTalk
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[201] or DestinationPort[201]))

#264: BGMP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[264] or DestinationPort[264]))

#318: TSP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[318] or DestinationPort[318]))

#381: HPOpenview
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[381] or DestinationPort[381]))

#382: HPOpenview
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[382] or DestinationPort[382]))

#383: HPOpenview
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[383] or DestinationPort[383]))

#389: LDAP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[389] or DestinationPort[389]))

#411: DirectConnect
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[411] or DestinationPort[411]))

#412: DirectConnect
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[412] or DestinationPort[412]))

#443: HTTPoverSSL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[443] or DestinationPort[443]))

#445: MicrosoftDS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[445] or DestinationPort[445]))

#464: Kerberos
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[464] or DestinationPort[464]))

#465: SMTPoverSSL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[465] or DestinationPort[465]))

#497: Retrospect
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[497] or DestinationPort[497]))

#500: ISAKMP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[500] or DestinationPort[500]))

#512: rexec
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[512] or DestinationPort[512]))

#513: rlogin
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[513] or DestinationPort[513]))
```

```
#514: syslog
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[514] or DestinationPort[514]))

#515: LPDLPR
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[515] or DestinationPort[515]))

#520: RIP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[520] or DestinationPort[520]))

#521: RIPngIPv6
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[521] or DestinationPort[521]))

#540: UUCP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[540] or DestinationPort[540]))

#554: RTSP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[554] or DestinationPort[554]))

#546: DHCPv6
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[546] or DestinationPort[546]))

#547: DHCPv6
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[547] or DestinationPort[547]))

#560: rmonitor
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[560] or DestinationPort[560]))

#563: NNTPoverSSL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[563] or DestinationPort[563]))

#587: SMTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[587] or DestinationPort[587]))

#591: FileMaker
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[591] or DestinationPort[591]))

#593: MicrosoftDCOM
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[593] or DestinationPort[593]))

#631: InternetPrinting
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[631] or DestinationPort[631]))

#636: LDAPoverSSL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[636] or DestinationPort[636]))

#639: MSDPPIM
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[639] or DestinationPort[639]))

#646: LDPMPLS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[646] or DestinationPort[646]))

#691: MSExchange
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[691] or DestinationPort[691]))
```

```
#860: iSCSI
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[860] or DestinationPort[860]))

#873: rsync
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[873] or DestinationPort[873]))

#902: VMwareServer
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[902] or DestinationPort[902]))

#989: FTPOverSSL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[989] or DestinationPort[989]))

#990: FTPoverSSL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[990] or DestinationPort[990]))

#993: IMAP4overSSL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[993] or DestinationPort[993]))

#995: POP3overSSL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[995] or DestinationPort[995]))

#1025: MicrosoftRPCORaim
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1025] or DestinationPort[1025]))

#1080: SOCKSProxyORMyDoom
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1080] or DestinationPort[1080]))

#1194: OpenVPN
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1194] or DestinationPort[1194]))

#1214: Kazaa
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1214] or DestinationPort[1214]))

#1241: Nessus
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1241] or DestinationPort[1241]))

#1311: DellOpenManage
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1311] or DestinationPort[1311]))

#1337: WASTE
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1337] or DestinationPort[1337]))

#1433: MicrosoftSQL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1433] or DestinationPort[1433]))

#1434: MicrosoftSQL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1434] or DestinationPort[1434]))

#1512: WINS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1512] or DestinationPort[1512]))

#1589: CiscoVQP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1589] or DestinationPort[1589]))
```

```
#1701: L2TP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1701] or DestinationPort[1701]))

#1723: MSPPTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1723] or DestinationPort[1723]))

#1725: Steam
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1725] or DestinationPort[1725]))

#1741: CiscoWorks2000
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1741] or DestinationPort[1741]))

#1755: MSMediaServer
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1755] or DestinationPort[1755]))

#1812: RADIUS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1812] or DestinationPort[1812]))

#1813: RADIUS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1813] or DestinationPort[1813]))

#1863: MSN
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1863] or DestinationPort[1863]))

#1985: CiscoHSRP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[1985] or DestinationPort[1985]))

#2000: CiscoSCCP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[2000] or DestinationPort[2000]))

#2002: CiscoACS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[2002] or DestinationPort[2002]))

#2049: NFS
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[2049] or DestinationPort[2049]))

#2100: OracleXDB
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[2100] or DestinationPort[2100]))

#2222: DirectAdmin
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[2222] or DestinationPort[2222]))

#2302: Halo
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[2302] or DestinationPort[2302]))

#2745: BagleH
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[2745] or DestinationPort[2745]))

#2967: SymantecAV
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[2967] or DestinationPort[2967]))

#3050: InterbaseDB
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3050] or DestinationPort[3050]))
```

```
#3074: XBOXLive
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3074] or DestinationPort[3074]))

#3124: HTTPProxy
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3124] or DestinationPort[3124]))

#3127: MyDoom
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3127] or DestinationPort[3127]))

#3128: HTTPProxy
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3128] or DestinationPort[3128]))

#3222: GLBP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3222] or DestinationPort[3222]))

#3260: iSCSITarget
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3260] or DestinationPort[3260]))

#3306: MySQL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3306] or DestinationPort[3306]))

#3389: TerminalServer
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3389] or DestinationPort[3389]))

#3689: iTunes
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3689] or DestinationPort[3689]))

#3690: Subversion
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3690] or DestinationPort[3690]))

#3724: WorldofWarcraft
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3724] or DestinationPort[3724]))

#4333: mSQL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[4333] or DestinationPort[4333]))

#4444: Blaster
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[4444] or DestinationPort[4444]))

#4664: GoogleDesktop
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[4664] or DestinationPort[4664]))

#4672: eMule
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[4672] or DestinationPort[4672]))

#4899: Radmin
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[4899] or DestinationPort[4899]))

#5000: UPnP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5000] or DestinationPort[5000]))

#5001: SlingboxORiperf
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5001] or DestinationPort[5001]))
```

```
#5004: RTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5004] or DestinationPort[5004]))

#5005: RTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5005] or DestinationPort[5005]))

#5050: YahooMessenger
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5050] or DestinationPort[5050]))

#5060: SIP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5060] or DestinationPort[5060]))

#5190: AIMICQ
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5190] or DestinationPort[5190]))

#5432: PostgreSQL
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5432] or DestinationPort[5432]))

#5500: VNCServer
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5500] or DestinationPort[5500]))

#5554: Sasser
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5554] or DestinationPort[5554]))

#5631: pcAnywhere
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5631] or DestinationPort[5631]))

#5632: pcAnywhere
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5632] or DestinationPort[5632]))

#5800: VNCoverHTTP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[5800] or DestinationPort[5800]))

#6112: Battlenet
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6112] or DestinationPort[6112]))

#6129: DameWare
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6129] or DestinationPort[6129]))

#6257: WinMX
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6257] or DestinationPort[6257]))

#6346: Gnutella
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6346] or DestinationPort[6346]))

#6347: Gnutella
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6347] or DestinationPort[6347]))

#6500: GameSpyArcade
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6500] or DestinationPort[6500]))

#6566: SANE
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6566] or DestinationPort[6566]))
```

```
#6588: AnalogX
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6588] or DestinationPort[6588]))

#6699: Napster
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6699] or DestinationPort[6699]))

#6970: Quicktime
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[6970] or DestinationPort[6970]))

#7212: GhostSurf
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[7212] or DestinationPort[7212]))

#8000: InternetRadio
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8000] or DestinationPort[8000]))

#8080: HTTPProxy
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8080] or DestinationPort[8080]))

#8086: KasperskyAV
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8086] or DestinationPort[8086]))

#8087: KasperskyAV
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8087] or DestinationPort[8087]))

#8118: Privoxy
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8118] or DestinationPort[8118]))

#8200: VMwareServer
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8200] or DestinationPort[8200]))

#8500: AdobeColdFusion
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8500] or DestinationPort[8500]))

#8767: TeamSpeak
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8767] or DestinationPort[8767]))

#8866: BagleB
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[8866] or DestinationPort[8866]))

#9100: HPJetDirect
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[9100] or DestinationPort[9100]))

#9119: MXit
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[9119] or DestinationPort[9119]))

#9800: WebDAV
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[9800] or DestinationPort[9800]))

#9898: Dabber
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[9898] or DestinationPort[9898]))

#9988: RbotSpybot
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[9988] or DestinationPort[9988]))
```

```
#9999: Urchin
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[9999] or DestinationPort[9999]))

#10000: WebminORBackupExec
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[10000] or DestinationPort[10000]))

#11371: OpenPGP
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[11371] or DestinationPort[11371]))

#12345: NetBus
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[12345] or DestinationPort[12345]))

#14567: Battlefield
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[14567] or DestinationPort[14567]))

#15118: DipnetOddbob
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[15118] or DestinationPort[15118]))

#19226: AdminSecure
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[19226] or DestinationPort[19226]))

#19638: Ensim
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[19638] or DestinationPort[19638]))

#20000: Usermin
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[20000] or DestinationPort[20000]))

#24800: Synergy
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[24800] or DestinationPort[24800]))

#25999: Xfire
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[25999] or DestinationPort[25999]))

#27015: HalfLife
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[27015] or DestinationPort[27015]))

#27374: Sub7
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[27374] or DestinationPort[27374]))

#28960: CallofDuty
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[28960] or DestinationPort[28960]))

#31337: BackOrifice
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[31337] or DestinationPort[31337]))


#3001: WWW
(Protocol[TCP] and ( SourcePort[80] or DestinationPort[80] or SourcePort[8080] or DestinationPor

#3002: FTP/P2P
(Protocol[TCP] and (DestinationPort[20-21] OR SourcePort[20-21]))

#3003: Mail
((Protocol[TCP] or Protocol[UDP]) and ( DestinationPort[143] or SourcePort[143] or DestinationPo
```

```
#3004: Chat
(Protocol[TCP] and (SourcePort[6667] or DestinationPort[6667])) OR (Protocol[TCP] and (SourcePor

#3005: Remote Control
((Protocol[TCP] or Protocol[UDP]) and (SourcePort[3389] or DestinationPort[3389])) OR (Protocol[

#3007: Infrastructure
(Protocol[UDP] and ((SourcePort[68] and DestinationPort[67]) or (SourcePort[67] and DestinationP

#3008: NetBIOS
((Protocol[TCP] OR Protocol[UDP]) AND (DestinationPort[137-139] OR SourcePort[137-139]))

#3009: Various
(Protocol[UDP]) OR (Protocol[TCP])

#1001: HTTP
Protocol[TCP] and ( SourcePort[80] or DestinationPort[80] or SourcePort[8080] or DestinationPort

#1023: HTTPS
Protocol[TCP] and (SourcePort[443] or DestinationPort[443])

#1024: FTP (Control)
Protocol[TCP] and (DestinationPort[20-21] OR SourcePort[20-21])

#1006: IMAP
(Protocol[TCP] or Protocol[UDP]) and ( DestinationPort[143] or SourcePort[143] or DestinationPor

#1008: POP3
Protocol[TCP] and (SourcePort[110] or DestinationPort[110] or SourcePort[995] or DestinationPort

#1011: SMTP
Protocol[TCP] and (SourcePort[25] or DestinationPort[25])

#1007: IRC
Protocol[TCP] and (SourcePort[6667] or DestinationPort[6667])

#1009: RDP
(Protocol[TCP] or Protocol[UDP]) and (SourcePort[3389] or DestinationPort[3389])

#1014: SSH
Protocol[TCP] and (SourcePort[22] or DestinationPort[22])

#1016: Telnet
Protocol[TCP] and (SourcePort[23] or DestinationPort[23])

#1017: VNC
Protocol[TCP] and (SourcePort[5800] or DestinationPort[5800] or SourcePort[5900] or DestinationP

#1003: DHCP
Protocol[UDP] and ((SourcePort[68] and DestinationPort[67]) or (SourcePort[67] and DestinationPo

#1004: DNS
(Protocol[TCP] or Protocol[UDP]) and (SourcePort[53] or DestinationPort[53])
```

```
#1005: Ident
Protocol[TCP] and (SourcePort[113] or DestinationPort[113])

#1018: ICMP
Protocol[ICMP]

#1012: SNMP
Protocol[TCP] and (SourcePort[161-162] or DestinationPort[161-162])

#1021: OtherUDP
Protocol[UDP]

#1022: OtherTCP
Protocol[TCP]
```

Revision #2
Created 19 May 2022 06:26:16 by Admin
Updated 23 May 2022 19:25:53 by Admin