WFPSampler Conditions for the Command Line

**See Also**

Filtering Conditions Available at Each Filtering Layer

|  |  |  |  |
| --- | --- | --- | --- |
| **FWPM\_CONDITION** | **Command line** **parameter** | **Acceptable value(s)** | **Example usage**  **<Condition> <MatchType> <Value>** |
| FWPM\_CONDITION\_INTERFACE\_MAC\_ADDRESS | -ima | MAC Address | -ima == 01:02:03:04:05:06 |
| FWPM\_CONDITION\_MAC\_LOCAL\_ADDRESS | -mla | MAC Address | -mla == 01:02:03:04:05:06 |
| FWPM\_CONDITION\_MAC\_REMOTE\_ADDRESS | -mra | MAC Address | -mra == 01:02:03:04:05:06 |
| FWPM\_CONDITION\_ETHER\_TYPE | -et | UINT16 | -et == 0x806 |
| NDIS\_ETH\_TYPE name | -et == NDIS\_ETH\_TYPE\_ARP |
| Well-known alias | -et == ARP |
| FWPM\_CONDITION\_VLAN\_ID | -vlid | UINT16 | -vlid == 0xFFFF |
| FWPM\_CONDITION\_VSWITCH\_TENANT\_NETWORK\_ID | -vstnid | UINT32 | -vstnid == 0xFFFFFFFF |
| FWPM\_CONDITION\_NDIS\_PORT | -np | UINT32 | -np == 0xFFFFFFFF |
| FWPM\_CONDITION\_NDIS\_MEDIA\_TYPE | -nmt | UINT32 | -nmt == 0 |
| NDIS\_MEDIUM name | -nmt == NdisMedium802\_3 |
| Well-known alias | -nmt == Ethernet |
| FWPM\_CONDITION\_PHYSICAL\_MEDIA\_TYPE | -npmt | UINT32 | -nmpt == 0x000E |
| NDIS\_PHYSICAL\_MEDIUM name | -nmpt == NdisPhysicalMedium802\_3 |
|  | -nmpt == Ethernet |
| FWPM\_CONDITION\_L2\_FLAGS | -l2f | UINT32 | -l2f == 0xA |
| FWPM\_CONDITION\_L2\_FLAG name | -l2f == FWP\_CONDITION\_L2\_IS\_WIFI |
| FWPM\_CONDITION\_MAC\_LOCAL\_ADDRESS\_TYPE | -mlat | UINT8 | -mlat == 0 |
| DL\_ADDRESS\_TYPE name | -mlat == DlUnicast |
| Well-known alias | -mlat == Unicast |
| FWPM\_CONDITION\_MAC\_REMOTE\_ADDRESS\_TYPE | -mrat | UINT8 | -mrat == 0 |
| DL\_ADDRESS\_TYPE name | -mrat == DlUnicast |
| Well-known alias | -mrat == Unicast |
| FWPM\_CONDITION\_ALE\_PACKAGE\_ID | -apid | SID | -apid == S-1-15-2-2551677095-2355568638-4209445997-2436930744-3692183382-387691378-1866284433 |
| Well-known alias | -apid == WinNullSid |
| FWPM\_CONDITION\_MAC\_SOURCE\_ADDRESS | -msa | MAC Address | -msa == 01:02:03:04:05:06 |
| FWPM\_CONDITION\_MAC\_DESTINATION\_ADDRESS | -mda | MAC Address | -mda == 01:02:03:04:05:06 |
| FWPM\_CONDITION\_MAC\_SOURCE\_ADDRESS\_TYPE | -msat | UINT8 | -msat == 0 |
| DL\_ADDRESS\_TYPE name | -msat == DlUnicast |
| Well-known alias | -msat == Unicast |
| FWPM\_CONDITION\_MAC\_DESTINATION\_ADDRESS\_TYPE | -mdat | UINT8 | -mdat == 0 |
| DL\_ADDRESS\_TYPE name | -mdat == DlUnicast |
| Well-known alias | -mdat == Unicast |
| FWPM\_CONDITION\_IP\_SOURCE\_PORT | -ipsp | UINT16 | -ipsp == 0xFFFF |
| FWPM\_CONDITION\_VSWITCH\_ICMP\_TYPE | -vsicmpt | UINT8 | -vsicmpt == 0xFF |
| FWPM\_CONDITION\_IP\_DESTINATION\_PORT | -ipdp | UINT16 | -ipdp == 0xFFFF |
| FWPM\_CONDITION\_VSWITCH\_ICMP\_CODE | -vsicmpc | UINT8 | -vsicmpc == 0xFF |
| FWPM\_CONDITION\_VSWITCH\_ID | -vsid | GUID | -vsid == 12345678-90AB-CDEF-1234-567890ABCDEF |
| FWPM\_CONDITION\_VSWITCH\_NETWORK\_TYPE | -vsnt | UINT8 | -vsnt == 3 |
| FWP\_VSWITCH\_NETWORK\_TYPE name | -vsnt == FWP\_VSWITCH\_NETWORK\_TYPE\_EXTERNAL |
| Well-known alias | -vsnt == External |
| FWPM\_CONDITION\_VSWITCH\_SOURCE\_INTERFACE\_ID | -vssiid | GUID(s) | -vssiid == 12345678-90AB-CDEF-1234-567890ABCDEF--12345678-90AB-CDEF-1234-567890ABCDEF |
| FWPM\_CONDITION\_VSWITCH\_DESTINATION\_INTERFACE\_ID | -vsdiid | GUID(s) | -vsdiid == 12345678-90AB-CDEF-1234-567890ABCDEF--12345678-90AB-CDEF-1234-567890ABCDEF |
| FWPM\_CONDITION\_VSWITCH\_SOURCE\_VM\_ID | -vssvmid | GUID | -vssvmid == 12345678-90AB-CDEF-1234-567890ABCDEF |
| FWPM\_CONDITION\_VSWITCH\_DESTINATION\_VM\_ID | -vsdvmid | GUID | -vsdvmid == 12345678-90AB-CDEF-1234-567890ABCDEF |
| FWPM\_CONDITION\_VSWITCH\_SOURCE\_INTERFACE\_TYPE | -vssit | UINT32 | -vssit == 0 |
| NDIS\_SWITCH\_NIC\_TYPE name | -vssit == SwitchNicTypeExternal |
| Well-known alias | -vssit == External |
| FWPM\_CONDITION\_VSWITCH\_DESTINATION\_INTERFACE\_TYPE | -vsdit | UINT32 | -vsdit == 0 |
| NDIS\_SWITCH\_NIC\_TYPE name | -vsdit == SwitchNicTypeExternal |
| Well-known alias | -vsdit == External |
| FWPM\_CONDITION\_ALE\_ORIGINAL\_APP\_ID | -aoaid | String | -aoaid == IExplore.Exe |
| FWPM\_CONDITION\_IP\_NEXTHOP\_ADDRESS | -ipnha | IPv4 Address | -ipnha == 1.2.3.4 |
| IPv6 Address | -ipnha == 1:2:3:4:5:6:7:8 |
| FWPM\_CONDITION\_ NEXTHOP\_SUB\_INTERFACE\_INDEX | -nhsii | UINT32 | -nhsii == 0xFFFFFFFF |
| FWPM\_CONDITION\_IP\_NEXTHOP\_INTERFACE | -ipnhi | UINT64 | -ipnhi == 0xFFFFFFFFFFFFFFFF |
| FWPM\_CONDITION\_NEXTHOP\_INTERFACE\_TYPE | -nhit | UINT32 | -nhit == 6 |
| IF\_TYPE name | -nhit == IF\_TYPE\_ETHERNET\_CSMACD |
| Well-known alias | -nhit == Ethernet |
| FWPM\_CONDITION\_NEXTHOP\_TUNNEL\_TYPE | -nhtt | UINT32 | -nhtt == 14 |
| TUNNEL\_TYPE name | -nhtt == TUNNEL\_TYPE\_TEREDO |
| Well-known alias | -nhtt == Teredo |
| FWPM\_CONDITION\_NEXTHOP\_INTERFACE\_INDEX | -nhii | UINT32 | -nhii == 0xFFFFFFFF |
| FWPM\_CONDITION\_ORIGINAL\_PROFILE\_ID | -opid | UINT32 | -opid == 1 |
| NL\_INTERFACE\_NETWORK\_CATEGORY\_STATE name | -opid == NlincPublic |
| Well-known alias | -opid == Public |
| FWPM\_CONDITION\_CURRENT\_PROFILE\_ID | -cpid | UINT32 | -cpid == 1 |
| NL\_INTERFACE\_NETWORK\_CATEGORY\_STATE name | -cpid == NlincPublic |
| Well-known alias | -cpid == Public |
| FWPM\_CONDITION\_LOCAL\_INTERFACE\_PROFILE\_ID | -lipid | UINT32 | -lipid == 1 |
| NL\_INTERFACE\_NETWORK\_CATEGORY\_STATE name | -lipid == NlincPublic |
| Well-known alias | -lipid == Public |
| FWPM\_CONDITION\_ARRIVAL\_INTERFACE\_PROFILE\_ID | -aipid | UINT32 | -aipid == 1 |
| NL\_INTERFACE\_NETWORK\_CATEGORY\_STATE name | -aipid == NlincPublic |
| Well-known alias | -aipid == Public |
| FWPM\_CONDITION\_NEXTHOP\_INTERFACE\_PROFILE\_ID | -nhipid | UINT32 | -nhipid == 1 |
| NL\_INTERFACE\_NETWORK\_CATEGORY\_STATE name | -nhipid == NlincPublic |
| Well-known alias | -nhipid == Public |
| FWPM\_CONDITION\_REAUTHORIZE\_REASON | -rr | UINT32 | -rr == 3 |
| FWP\_CONDITION\_REAUTHORIZE\_REASON name | -rr == FWP\_CONDITION\_REAUTHORIZE\_REASON\_POLICY\_CHANGE |
| Well-known alias | -rr == PolicyChange |
| FWPM\_CONDITION\_ORIGINAL\_ICMP\_TYPE | -oicmpt | UINT16 | -oicmpt == 0xFF |
| FWPM\_CONDITION\_IP\_PHYSICAL\_ARRIVAL\_INTERFACE | -ippai | UINT64 | -ippai == 0xFFFFFFFFFFFFFFFF |
| FWPM\_CONDITION\_IP\_PHYSICAL\_NEXTHOP\_INTERFACE | -ippnhi | UINT64 | -ippnhi == 0xFFFFFFFFFFFFFFFF |
| FWPM\_CONDITION\_INTERFACE\_QUARANTINE\_EPOCH | -iqe | UINT64 | -iqe == 0xFFFFFFFFFFFFFFFF |
| FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS | -ipla | IPv4 Address | -ipla == 1.2.3.4 |
| IPv6 Address | -ipla == 1:2:3:4:5:6:7:8 |
| FWPM\_CONDITION\_IP\_REMOTE\_ADDRESS | -ipra | IPv4 Address | -ipra == 1.2.3.4 |
| IPv6 Address | -ipra == 1:2:3:4:5:6:7:8 |
| FWPM\_CONDITION\_IP\_SOURCE\_ADDRESS | -ipsa | IPv4 Address | -ipsa == 1.2.3.4 |
| IPv6 Address | -ipsa == 1:2:3:4:5:6:7:8 |
| FWPM\_CONDITION\_IP\_DESTINATION\_ADDRESS | -ipda | IPv4 Address | -ipda == 1.2.3.4 |
| IPv6 Address | -ipda == 1:2:3:4:5:6:7:8 |
| FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS\_TYPE | -iplat | UINT8 | -iplat == 1 |
| NL\_ADDRESS\_TYPE name | -iplat == NlatUnicast |
| Well-known alias | -iplat == Unicast |
| FWPM\_CONDITION\_IP\_DESTINATION\_ADDRESS\_TYPE | -ipdat | UINT8 | -ipdat == 1 |
| NL\_ADDRESS\_TYPE name | -ipdat == NlatUnicast |
| Well-known alias | -ipdat == Unicast |
| FWPM\_CONDITION\_IP\_LOCAL\_INTERFACE | -ipli | UINT64 | -ipli == 0xFFFFFFFFFFFFFFFF |
| FWPM\_CONDITION\_IP\_INTERFACE | -ipi | UINT64 | -ipi == 0xFFFFFFFFFFFFFFFF |
| FWPM\_CONDITION\_IP\_ARRIVAL\_INTERFACE | -ipai | UINT64 | -ipai == 0xFFFFFFFFFFFFFFFF |
| FWPM\_CONDITION\_ARRIVAL\_INTERFACE\_TYPE | -ait | UINT32 | -ait == 6 |
| IF\_TYPE name | -ait == IF\_TYPE\_ETHERNET\_CSMACD |
| Well-known alias | -ait == Ethernet |
| FWPM\_CONDITION\_ARRIVAL\_TUNNEL\_TYPE | -att | UINT32 | -att == 14 |
| TUNNEL\_TYPE name | -att == TUNNEL\_TYPE\_TEREDO |
| Well-known alias | -att == Teredo |
| FWPM\_CONDITION\_ARRIVAL\_INTERFACE\_INDEX | -aii | UINT32 | -aii == 0xFFFFFFFF |
| FWPM\_CONDITION\_INTERFACE\_TYPE | -it | UINT32 | -it == 6 |
| IF\_TYPE name | -it == IF\_TYPE\_ETHERNET\_CSMACD |
| Well-known alias | -it == Ethernet |
| FWPM\_CONDITION\_LOCAL\_INTERFACE\_TYPE | -lit | UINT32 | -lit == 6 |
| IF\_TYPE name | -lit == IF\_TYPE\_ETHERNET\_CSMACD |
| Well-known alias | -lit == Ethernet |
| FWPM\_CONDITION\_TUNNEL\_TYPE | -tt | UINT32 | -tt == 14 |
| TUNNEL\_TYPE name | -tt == TUNNEL\_TYPE\_TEREDO |
| Well-known alias | -tt == Teredo |
| FWPM\_CONDITION\_LOCAL\_TUNNEL\_TYPE | -ltt | UINT32 | -ltt == 14 |
| TUNNEL\_TYPE name | -ltt == TUNNEL\_TYPE\_TEREDO |
| Well-known alias | -ltt == Teredo |
| FWPM\_CONDITION\_IP\_FORWARD\_INTERFACE | -ipfi | UINT64 | -ipfi == 0xFFFFFFFFFFFFFFFF |
| FWPM\_CONDITION\_IP\_PROTOCOL | -ipp | UINT8 | -ipp == 6 |
| Well-known alias | -ipp == TCP |
| FWPM\_CONDITION\_IP\_LOCAL\_PORT | -iplp | UINT16 | -iplp == 0xFFFF |
| FWPM\_CONDITION\_ICMP\_TYPE | -icmpt | UINT8 | -icmpt == 0xFF |
| FWPM\_CONDITION\_IP\_REMOTE\_PORT | -iprp | UINT16 | -iprp == 0xFFFF |
| FWPM\_CONDITION\_ICMP\_CODE | -icmpc | UINT8 | -icmpc == 0xFF |
| FWPM\_CONDITION\_EMBEDDED\_LOCAL\_ADDRESS\_TYPE | -elat | UINT8 | -elat == 1 |
| NL\_ADDRESS\_TYPE name | -elat == NlatUnicast |
| Well-known alias | -elat == Unicast |
| FWPM\_CONDITION\_EMBEDDED\_REMOTE\_ADDRESS | -era | IPv4 Address | -era == 1.2.3.4 |
| IPv6 Address | -era == 1:2:3:4:5:6:7:8 |
| FWPM\_CONDITION\_EMBEDDED\_PROTOCOL | -ep | UINT8 | -ep == 6 |
| Well-known alias | -ep == TCP |
| FWPM\_CONDITION\_EMBEDDED\_LOCAL\_PORT | -elp | UINT16 | -elp == 0xFFFF |
| FWPM\_CONDITION\_EMBEDDED\_REMOTE\_PORT | -erp | UINT16 | -erp == 0xFFFF |
| FWPM\_CONDITION\_FLAGS | -f | UINT32 | -f == 3 |
| FWP\_CONDITION\_FLAG name | -f == FWP\_CONDITION\_FLAG\_IS\_IPSEC\_SECURED |
| FWPM\_CONDITION\_DIRECTION | -d | UINT | -d == 0 |
| FWP\_DIRECTION name | -d == FWP\_DIRECTION\_OUTBOUND |
| Well-known alias | -d == Outbound |
| FWPM\_CONDITION\_ INTERFACE\_INDEX | -ii | UINT32 | -ii == 0xFFFFFFFF |
| FWPM\_CONDITION\_LOCAL\_INTERFACE\_INDEX | -lii | UINT32 | -lii == 0xFFFFFFFF |
| FWPM\_CONDITION\_SUB\_INTERFACE\_INDEX | -subii | UINT32 | -subii == 0xFFFFFFFF |
| FWPM\_CONDITION\_ARRIVAL\_SUB\_INTERFACE\_INDEX | -asii | UINT32 | -asii == 0xFFFFFFFF |
| FWPM\_CONDITION\_SOURCE\_INTERFACE\_INDEX | -sii | UINT32 | -sii == 0xFFFFFFFF |
| FWPM\_CONDITION\_SOURCE\_SUB\_INTERFACE\_INDEX | -ssii | UINT32 | -ssii == 0xFFFFFFFF |
| FWPM\_CONDITION\_DESTINATION\_INTERFACE\_INDEX | -dii | UINT32 | -dii == 0xFFFFFFFF |
| FWPM\_CONDITION\_DESTINATION\_SUB\_INTERFACE\_INDEX | -dsii | UINT32 | -dsii == 0xFFFFFFFF |
| FWPM\_CONDITION\_ALE\_APP\_ID | -aaid | String | -aaid == IExplore.exe |
| FWPM\_CONDITION\_ALE\_USER\_ID | -auid | String | -auid == Domain\UserName |
| FWPM\_CONDITION\_REMOTE\_USER\_ID | -aruid | String | -aruid == Domain\UserName |
| FWPM\_CONDITION\_REMOTE\_MACHINE\_ID | -armid | String | -armid == MachineName |
| FWPM\_CONDITION\_PROMISCUOUS\_MODE | -apm | UINT32 | -apm == 1 |
| FWPM\_CONDITION\_ALE\_SIO\_FIREWALL\_SYSTEM\_PORT | -asfsp | UINT32 | -asfsp == 1 |
| FWPM\_CONDITION\_ALE\_SIO\_FIREWALL\_SOCKET\_PROPERTY | -asfsp | UINT32 | -asfsp == 1 |
| FWPM\_CONDITION\_ALE\_NAP\_CONTEXT | -anc | UINT32 | -anc == 0xFFFFFFFF |
| FWPM\_CONDITION\_REMOTE\_USER\_TOKEN |  |  |  |
| FWPM\_CONDITION\_RPC\_IF\_UUID |  |  |  |
| FWPM\_CONDITION\_IF\_VERSION | -riv | UINT16 | -riv == 0xFFFF |
| FWPM\_CONDITION\_RPC\_IF\_FLAG | -rif | UINT32 | -rif == 1 |
| Well-known alias | -rif == RPC\_FW\_IF\_FLAG\_DCOM |
| FWPM\_CONDITION\_DCOM\_APP\_ID |  |  |  |
| FWPM\_CONDITION\_IMAGE\_NAME |  |  |  |
| FWPM\_CONDITION\_RPC\_PROTOCOL | -rp | UINT8 | -rp == 7 |
| Well-known alias | -rp == NCACN\_IP\_TCP |
| FWPM\_CONDITION\_RPC\_AUTH\_TYPE | -rat | UINT8 | -rat == 0 |
| Well-known alias | -rat ==  RPC\_C\_AUTHN\_NONE |
| FWPM\_CONDITION\_RPC\_AUTH\_LEVEL | -ral | UINT8 | -ral == 0 |
| Well-known alias | -ral ==  RPC\_C\_AUTHN\_LEVEL\_DEFAULT |
| FWPM\_CONDITION\_SEC\_ENCRYPT\_ALGORITHM | -sea | UINT32 | -sea == 1 |
| FWPM\_CONDITION\_SEC\_KEY\_SIZE | -sks | UINT32 | -sks == 128 |
| FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS\_V4 | -iplav4 | IPv4 Address | -iplav4 == 1.2.3.4 |
| FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS\_V6 | -iplav6 | IPv6 Address | -iplav6 == 1:2:3:4:5:6:7:8 |
| FWPM\_CONDITION\_PIPE |  |  |  |
| FWPM\_CONDITION\_IP\_REMOTE\_ADDRESS\_V4 | -iprav4 | Ipv4 Address | -Iprav4 == 1.2.3.4 |
| FWPM\_CONDITION\_IP\_REMOTE\_ADDRESS\_V6 | -iprav6 | IPv6 Address | -iprav6 == 1:2:3:4:5:6:7:8 |
| FWPM\_CONDITION\_PROCESS\_WITH\_RPC\_IF\_UUID |  |  |  |
| FWPM\_CONDITION\_RPC\_EP\_VALUE |  |  |  |
| FWPM\_CONDITION\_RPC\_EP\_FLAGS | -ref | UINT32 | -ref == 1 |
| Well-known alias | -ref == RPC\_FW\_IF\_FLAG\_DCOM |
| FWPM\_CONDITION\_RPC\_SERVER\_NAME |  |  |  |
| FWPM\_CONDITION\_RPC\_SERVER\_PORT | -rsp | UINT16 | -rsp == 1 |
| FWPM\_CONDITION\_RPC\_PROXY\_AUTH\_TYPE |  |  |  |
| FWPM\_CONDITION\_CLIENT\_CERT\_KEY\_LENGTH | -cckl | UINT32 | -cckl == 128 |
| FWPM\_CONDITION\_CLIENT\_CERT\_OID |  |  |  |
| FWPM\_CONDITION\_NET\_EVENT\_TYPE |  |  |  |
| FWPM\_CONDITION\_KM\_AUTH\_NAP\_CONTEXT | -kanc | UINT32 | -kanc == 1 |
| FWPM\_CONDITION\_PEER\_NAME |  |  |  |
| FWPM\_CONDITION\_REMOTE\_ID |  |  |  |
| FWPM\_CONDITION\_AUTHENTICATION\_TYPE | -at | UINT32 | -at == 1 |
| FWPM\_CONDITION\_KM\_TYPE | -kt | UINT32 | -kt == 1 |
| FWPM\_CONDITION\_KM\_MODE | -km | UINT32 | -km == 1 |
| FWPM\_CONDITION\_IPSEC\_POLICY\_KEY |  |  |  |
| FWPM\_CONDITION\_QM\_MODE | -qm | UINT32 | -qm == 1 |
| FWPM\_CONDITION\_IPSEC\_SECURITY\_REALM\_ID | -isrid | String | -isrid == “MyIPsecSecurityRealm” |
| FWPM\_CONDITION\_ALE\_SECURITY\_ATTRIBUTE\_FQBN\_VALUE | -asafv | String | -asafv == “” |