Personal Firewall Default Rules and Components

https://campus.barracuda.com/doc/46895322/

The Barracuda Personal Firewall comes with a default access ruleset. The following tables aim to give you a compact overview of the default rules and their functions.

Rule Categories

The default rules are split into the following rule categories:

Main Category	Sub Category Level #1	Sub Category Level #2
Lockdown	Block all outbound and inbound traffic	
Mixed (default)	Allow outbound and inbound	Core network
	Barracuda VPN Allow Outbound and Inbound (Only on Adapter [TRUSTED])	Network Discovery
		Ipv6 Tunnel
		File and Printer Sharing (only on MY Net)
WLAN	Allow outbound and inbound	Core network
	Allow outbound	Barracuda VPN
		IPv6 tunnel
		File and printer sharing (only on my net)
	Block inbound	Network discovery
		File and printer sharing
	Block outbound	Network discovery
Domain	Allow outbound and inbound	
	Barracuda VPN	
	Network discovery	
	Core network	
	IPv6 tunnel	
	File and printer sharing (only on my net)	

Adapters

The following tables show the adapter denominations used and what they mean.

DYNAMIC

Name	Description
All System Adapters	Examples: • **VPN Network** • **Wireless Network Connection** • **Local Area Connection** • **Mobile Broadband Connection** • **Reusable Microsoft 6To4 Adapter** • **Teredo Tunneling pseudo interface**

DYNAMIC [isatap]

Name	Description
Intra-Site Automatic Tunneling Addressing Protocol	ISATAP uses IPv4 as a virtual nonbroadcast multiple-access network (NBMA) data link layer, so that it does not require the underlying IPv4 network infrastructure to support multicast. Example: **isatap.{09D450D7-FDBA-4B29-8165-5ED2EAB69606}**

DYNAMIC [multi]

Name	Description
Adapter [TRUSTED]	All trusted adapters: • **Ips: mc (managed by CC)** • **Barracuda VPN Adapter** • **Ethernet Adapter** • **Ask User and click “trusted”**
Adapter [TUNNEL]	All OS tunneling adapters
Adapter [Dial-up]	Dial-up adapter, e.g. a modem
Adapter [Ethernet]	Ethernet based adapters
Adapter [PolSrv]	Adapter that was used for the last Access Control Service connection
Adapter [UNTRUSTED]	All untrusted adapters: • **Wireless adapter** • **Dial-up adapter**
Adapter [Virtual]	Virtual adapters
Adapter [VPN]	Barracuda virtual adapter
Adapter [Wireless]	Wireless adapters

Networks

The following tables show the network denominations used and what they mean.

DYNAMIC

Name	Description
Any	`::/0, 0.0.0.0`
localIP	All local IP addresses
localPolicyIP	Local IP connect to Access Control Service
localTrustedIP	All local IP addresses from trusted adapters
Net-Personal VPN	All Barracuda client secure personal routes
TrustedNet	Secure zone
UntrustedNet	Insecure zone
virtualIP	All Barracuda VPN IP addresses

DYNAMIC [net]

Name	Description
Link-local	`::fe80::/64` Secure Link-local Zone

Link-Local Scope Multicast Addresses	`ff02::1, ff02::2, ff02::16, ff02::1:3`
	`Ref: Solicited-Node Multicast Addresses`

Net-Broadcast	`255.255.255.255` All Broadcast
Node-Local Scope Multicast Addresses	`ff01::2, ff01::1`
Simple Service Discovery Protocol	`ff0e::8, ff05::8, ff05::c, ff02::c, 239.255.255.250` Well-known practical multicast addresses for SSDP
Site-Local Scope Multicast Addresses	`ff05::1:3, ff05::2`
Solicited-Node Multicast Addresses	The solicited-node multicast address facilitates the efficient querying of network nodes during address resolution
Net-[Adapter Name]	

LOCAL

Name	Description

LLMRN	
MY Net	`Ref: TrustedNet` My private trusted network

SSDP	`Ref: Simple Service Discovery Protocol`
	`Ref: MY Net`

Services

This table shows the services you can choose from, as well as their protocols, default ports, and function.

Name	Port	Description
Barracuda VPN	• 691 TCP & UDP • 443 TCP-IPHTTPS • 3128 TCP - Squid Proxy • 8080 TCP - MS Proxy • 500 UDP - IPsec • 53 UDP - DNS	Barracuda VPN Tunnel
BOOTPS	• 67 Bootstrap Protocol Client • 68 Bootstrap Protocol Server	Bootstrap Protocol
CIFS	• 445 UDP • 445 TCP	Microsoft Windows 2000 SMB
DHCPv6	• 546 UDP-DHCPv6 Client • 547 UDP-DHCPv6 Server	DHCPv6 [RFC 3315]
DNS	• 53 UDP	Domain Name resolution
ICMP Echo	• ICMP 0 (Echo reply) • ICMP 8 (Echo request) • ICMPv6 128 (Echo request [RFC 4443]) • ICMPv6 129 (Echo reply [RFC 4443])	ipv6 and ipv4 Echo reply and request
ICMPv6 Multicast Listener Discovery	• 130 Multicast Listener Query [RFC 2710] • 131 Multicast Listener Report [RFC 2710] • 132 Multicast Listener Done [RFC 2710] • 143 Version 2 Multicast Listener Report [RFC 3810]	

ICMPv6 Neighbor Discovery	• 133 Router Solicitation [RFC 4861] • 135 Neighbor Solicitation [RFC 4861] • 136 Neighbor Advertisement [RFC 4861] • 137 Redirect Message [RFC 4861]	
ICMPv6 Router Advertisement	134 ICMPv6	Router Advertisement [RFC 4861]
IGMP	Protocol 2	Internet Group Message Protocol
IPv6 over IPv4	Protocol 41	IPv6 over IPv4
IPv6-noNxt	Protocol 59	IPv6 No Next Header
LLMNR	5355 UDP	Link-Local Multicast, allows hosts to perform name resolution for host on the same local link
NETBIOS-DBM	• 138 UDP • 138 TCP	NETBIOS Datagram Service
NETBIOS-NS	• 137 UDP • 137 TCP	NETBIOS Name Service
NETBIOS-SSN	• 139 UDP • 139 TCP	NETBIOS Session Service
POLSRV	44000 TCP	Barracuda CloudGen Network Access Control Service
SSDP	• 1900 UDP Simple Service Discovery Protocol • 2869 TCP SSDP event notification • 5000 TCP SSDP legacy event notification	Simple Service Discovery Protocol. Enables discovery of UPnP devices
WEB	80, 8080, 3128 TCP Ref: IPHTTPS (443 TCP)	
WS-Discovery	3702 TCP & UDP	Web Services Dynamic Discovery is a technical specification that defines a multicast discovery protocol to locate services on a local network.

Applications

This table shows the applications known by default to the Barracuda Personal Firewall.

Name	*.*	Description

EXPLORER	explorer.exe	Windows Explorer
LSASS	• LSASS.EXE (Local Security Authority Process) • TASKHOST.EXE (Host Process for Windows Tasks)	
POLSRV	phionha.exe	Barracuda CloudGen Health Agent
SSDP	• SVCHOST.EXE • WMPNETWK.EXE (Windows Media Player)	Network-Discovery
SVCHOST	SVCHOST.EXE	Host Process for Windows Services

Personal Firewall Default Rules

The following tables provide an overview of the default rules and their functions.

Changes in sections other than **Local** may impact the functionality of the OS.

Barracuda VPN

The rules in this section are used for VPN server connections and for filtering content within tunnels.

Outbound

Tunnel – Outbound Barracuda VPN Tunnel

Adapter	
Source	localIP
Destination	Any
Service	Barracuda VPN
Application	BARRACUDA VPN (phions.exe)
Settings	**Core Network > Barracuda VPN** **• Yes (default)** **• No**

Payload – Outbound Barracuda VPN Payload

Adapter	Adapter [VPN]
Source	
Destination	*
Service	Any

Application	Any
Settings	**Core Network > Barracuda VPN** **• Yes (default)** **• No**

* Possible **Network** objects to restrict the traffic:

- **Net-Personal VPN**: All Barracuda Client Secure Routes
- **Net-VPN Network**: Dynamic Virtual Dapter Object

Network Discovery

These rules are used to allow or restrict device, service, or machine discovery functionalities on the network.

Outbound

Network Discovery (WSD) – Outbound rule for Network Discovery to discover devices via Function Discovery

Adapter	Adapter [TRUSTED]
Source	Any
Destination	Any
Service	WS-Discovery
Application	SVCHOST

Network Discovery (LLMNR) – Outbound rule for Network Discovery to allow Link Local Multicast Name Resolution

Adapter	Adapter [TRUSTED] BLOCK on Mismatch
Source	localIP
Destination	LLMNR
Service	LLMNR
Application	SVCHOST

Network Discovery (SSDP) – Outbound rule for Network Discovery to allow use of the Simple Service Discovery Protocol

Adapter	Adapter [TRUSTED] BLOCK on Mismatch

Source	Any
Destination	SSDP
Service	SSDP
Application	SSDP

Inbound

Network Discovery (LLMNR) – Inbound rule for Network Discovery to allow Link Local Multicast Name Resolution

Adapter	Adapter [TRUSTED] BLOCK on Mismatch
Source	LLMNR
Destination	LLMNR
Service	LLMNR
Application	SVCHOST

Network Discovery (WSD) – Inbound rule for Network Discovery to discover devices via Function Discovery

Adapter	Adapter [TRUSTED] BLOCK on Mismatch
Source	Any
Destination	Any
Service	WS-Discovery
Application	SVCHOST

Network Discovery (SSDP) – Outbound rule for Network Discovery to allow use of the Simple Service Discovery Protocol

Adapter	Adapter [TRUSTED] BLOCK on Mismatch
Source	Any
Destination	SSDP
Service	SSDP
Application	SSDP

Core Network

These rules are for managing the core network. They abstract the most common protocols and functionalities, such as address assignment, group policy assignment, address lookup, and IPv6 auto-configuration as well as operating system and certificate updates. Also included is a rule to allow or restrict the system’s access to the Barracuda Access Control Server.

Outbound

Core Network - Dynamic Host Configuration – Allows DHCP messages for stateful auto-configuration

Adapter	
Source	0.0.0.0/0
Destination	0.0.0.0/0
Service	BOOTPS
Application	Any

Core Network - Dynamic Host Configuration for IPv6 – Allows DHCPv6 messages for stateful and stateless configuration

Adapter	
Source	Any
Destination	Any
Service	DHCPv6
Application	Any

Core Network - Router Advertisement Guard – Router Advertisement (RA) messages are used by routers to announce themselves on the link. The IPv6 Router Advertisement Guard can analyze and filter these RA messages.

Adapter	
Source	Any
Destination	Any
Service	ICMPv6 Router Advertisement
Application	Any

Core Network - Neighbor Discovery – Neighbor Discovery Solicit and Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.

Adapter	
Source	Any

Destination	Any
Service	ICMPv6 Neighbor Discovery
Application	ICMPv6

Core Network - Multicast Listener Report – The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.

Adapter	
Source	Any
Destination	Any
Service	ICMPv6 Multicast Listener Discovery
Application	Any

Core Network - Group Policy – Outbound rule to allow remote LSASS trafic for Group Policy updates

Adapter	
Source	Any
Destination	Any
Service	Any
Application	LSASS

Core Network - IPv6 No Next Header – The **Next Header** field indicates that there is no next header whatsoever following this one, not even a header of an upper-layer protocol.

Adapter	
Source	Any
Destination	Link-Local Scope Multicast Addresses
Service	Ipv6-NoNxt
Application	*

Core Network - DNS – Outbound rule to allow DNS requests. DNS responses based on requests that matched this rule will be permitted regardless of their source address.

Adapter	
Source	Any
Destination	Any
Service	DNS
Application	SVCHOST

Core Network - Internet Group Management Protocol – IGMP messages are sent and received by nodes to create, join, or depart multicast groups.

Adapter	
Source	Any
Destination	Any
Service	IGMP
Application	*

Core Network - Update Service – Outbound rule to allow Windows, certificate, and CRL updates.

Adapter	
Source	Any
Destination	Any
Service	WEB
Application	SVCHOST

Core Network - Group Policy (TCP-Out) – Outbound rule to allow remote RPC traffic for Group Policy updates

Adapter	Adapter [TRUSTED]
Source	Any
Destination	Any
Service	TCP*
Application	SVCHOST

Core Network - Group Policy (UDP-Out) – Outbound rule to allow remote PRC traffic for Group Policy updates

Adapter	Adapter [TRUSTED]
Source	Any
Destination	Any
Service	UDP*
Application	SVCHOST

Core Network - Explorer – Windows Explorer

Adapter	
Source	Any

Destination	MY Net
Service	Any
Application	EXPLORER

Core Network - Access Control Service – Barracuda CloudGen Network Access Control Service

Adapter	
Source	localIP
Destination	Any
Service	POLSRV
Application	POLSRV

Core Network - Dynamic Host Configuration – Allows DHCP messages for stateful auto-configuration

Adapter	
Source	0.0.0.0/0
Destination	0.0.0.0/0
Service	BOOTPS
Application	Any

Core Network - Dynamic Host Configuration for IPv6 – Allows DHCPv6 messages for stateful and stateless configuration

Adapter	
Source	Any
Destination	Any
Service	DHCPv6
Application	Any

Core Network - Router Advertisement Guard – Analyzes and filters Router Advertisement messages

Adapter	
Source	Any
Destination	Any
Service	ICMPv6 Router Advertisement
Application	Any

Settings	**Core Network > IPv6 RA Guard** **• Block all RA (default)** **• Disable** **• IPv6 Prefixes**

Core Network - Neighbor Discovery – Neighbor Discovery Solicit and Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.

Adapter	
Source	Any
Destination	Any
Service	ICMPv6 Neighbor Discovery
Application	ICMPv6

Core Network - Multicast Neighbor Discovery – Neighbor Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.

Adapter	
Source	Any
Destination	Link-Local Multicast Addresses
Service	ICMPv6 Neighbor Discovery
Application	ICMPv6

Core Network - Multicast Listener Report – The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.

Adapter	
Source	Any
Destination	Any
Service	ICMPv6 Multicast Listener Discovery
Application	ICMPv6

Core Network - Internet Group Management Protocol – IGMP messages are sent and received by nodes to create, join ,or depart multicast groups.

Adapter	
Source	Any

Destination	Any
Service	IGMP
Application	*

Core IPv6 Tunnel

These rules allow management of the tunnel traffic for the two IPv6 tunneling protocols that are active by default, e.g. ,in Windows 7.

Outbound

Core IPv6 Tunnel - Teredo (UDP-Out) – Outbound UDP rule to allow Teredo edge traversal

Adapter	Adapter [TUNNEL]
Source	0.0.0.0/0
Destination	Any
Service	UDP *
Application	SVCHOST
Settings	**Core Network > Teredo Tunnel** **• Yes (default)** **• No**

Core IPv6 Tunnel - IPv6 over IPv4 – Outbound IPv6 over IPv6 tunneling allows access to the IPv6 Internet in absence of an IPv6 native access provider

Adapter	
Source	localIP
Destination	Any
Service	IPv6 over IPv4
Application	Any
Settings	**Core Network > IPv6 over IPv4** **• Yes (default)** **• No**

File and Printer Sharing

These rules are for managing access to printers, files, and folders shared over the network.

Outbound

File and Printer Sharing - Echo Request – Echo request messages are sent as ping requests to other nodes.

Adapter	
Source	localIP
Destination	MY Net
Service	ICMP Echo
Application	*
Settings	**File and Printer Sharing > Outbound** **• Yes (default)** **• No**

File and Printer Sharing - NB-Name-Out – Outbound rule for File and Printer Sharing to allow NetBIOS Name Resolution

Adapter	Adapter [TRUSTED]
Source	localIP
Destination	MY Net
Service	NETBIOS-NS
Application	SYSTEM
Settings	**File and Printer Sharing > Outbound** **• Yes (default)** **• No**

File and Printer Sharing - NB-Datagram-Out Outbound rule for File and Printer Sharing to allow NetBIOS Datagram transmission and reception

Adapter	Adapter [TRUSTED]
Source	localIP
Destination	MY Net
Service	NETBIOS-DMB
Application	SYSTEM
Settings	**File and Printer Sharing > Outbound** **• Yes (default)** **• No**

Outbound rule for File and Printer Sharing to allow NetBIOS Session Service connections

Adapter	Adapter [TRUSTED]
Source	localIP
Destination	MY Net

Service	NETBIOS-SSN
Application	SYSTEM
Settings	**File and Printer Sharing > Outbound** **• Yes (default)** **• No**

File and Printer Sharing - SMB-Out Outbound rule for File and Printer Sharing to allow Server Message Block transmission and reception via Named Pipes

Adapter	Adapter [TRUSTED]
Source	Any
Destination	MY Net
Service	CIFS
Application	SYSTEM
Settings	**File and Printer Sharing > Outbound** **• Yes (default)** **• No**

File and Printer Sharing - NB-Name-Out Outbound rule for File and Printer Sharing to allow NetBIOS Name Resolution

Adapter	Adapter [TRUSTED]
Source	localIP
Destination	MY Net
Service	NETBIOS-NS
Application	SYSTEM
Settings	**File and Printer Sharing > Outbound** **• Yes (default)** **• No**

Inbound

File and Printer Sharing - NB-Datagram-In Outbound rule for File and Printer Sharing to allow NetBIOS Datagram transmission and reception

Adapter	Adapter [TRUSTED]
Source	MY Net
Destination	MY Net
Service	NETBIOS-DGM
Application	SYSTEM

Settings	**File and Printer Sharing > Inbound** **• Yes (default)** **• No**

File and Printer Sharing - NB-Name-In Inbound rule for File and Printer Sharing to allow NetBIOS Name Resolution

Adapter	Adapter [TRUSTED]
Source	MY Net
Destination	MY Net
Service	NETBIOS-NS
Application	SYSTEM
Settings	**File and Printer Sharing > Inbound** **• Yes (default)** **• No**

File and Printer Sharing - NB-Session-In Outbound rule for File and Printer Sharing to allow NetBIOS Session Service connections

Adapter	Adapter [TRUSTED]
Source	MY Net
Destination	MY Net
Service	NETBIOS-SSN
Application	SYSTEM
Settings	**File and Printer Sharing > Inbound** **• Yes (default)** **• No**

File and Printer Sharing - SMB-In Outbound rule for File and Printer Sharing to allow Server Message Block transmission and reception via Named Pipes

Adapter	Adapter [TRUSTED]
Source	MY Net
Destination	localIP
Service	CIFS
Application	SYSTEM
Settings	**File and Printer Sharing > Inbound** **• Yes (default)** **• No**

Local

These are custom defined rules for other applications, networks, and network locations.

Outbound

Internet

Adapter	
Source	localIP
Destination	Any
Service	WEB
Application	Any
Settings	**Internet > Web access** **• Yes (default)** **• No**