Check Point Ports list

WEB: https://martin.frlicka.net

Copyright © 2021 Martin Frlicka v1.5

Security Management | Firewall | Infrastructure | Clustering | IPsec VPN / SecuRemote / SecureClient | Endpoint Security | Mobile Access | Antivirus | Anti-Spam | URL Filtering | Identity Awareness | Data Loss Prevention DLP | Threat Emulation | Eventia Analyzer / Reporting | UTM-1 Edge

TCP	80	*not predefined*	Client -> Policy Server communication (over HTTP): Policy download, Anti-Malware updates, Client package, Application Control
TCP	80	*not predefined*	Client -> Policy Server communication (encrypted ESP): Sync request, heartbeat, log upload
TCP	81	*not predefined*	Used on Endpoint Security Management Server for CPTNL proxy -> Apache communication
UDP	161	*SNMP-GET* - Check Point Security Gateway SNMP Agent	A request for information sent by the SNMP server
UDP	162	*SNMP-TRAP* - Check Point Security Gateway SNMP Agent	Traps are initiated in case of an event on the monitored gateway
TCP	256	*FW1* - Check Point Security Gateway Service	Connections to Security Gateway Service (to FWD daemon): - Fetching topology information by Security Gateway (by FWD daemon) from Security Management Server or Domain Management Server (CMA) - Full Synchronization between cluster members (by FWD daemons) Used by the following commands: fw isp_link <server_ip> fw getver <server_ip> fw logswitch -h <server_ip> fw lslogs <server_ip> fw fetchlogs <server_ip> IPS packet capture
TCP	257	*FW1_log* - Check Point Security Gateway Logs	Delivering logs from Security Gateway (by FWD daemon) to Security Management Server / Customer Management Add-on (CMA) / Domain Management Server / Customer Log Module (CLM) / Domain Log Server
TCP	258	*FW1_mgmt* - Check Point Security Management (Version 4.x)	Communication between SmartConsole applications and Security Management Server (by FWM daemon)
TCP	259	*FW1_clntauth_telnet* - Check Point Security Gateway Client Authentication	Client Authentication on Security Gateway (*in.aclientd* daemon) using Telnet
UDP	259	RDP - Check Point Security Gateway FWZ Key Negotiations. Note: Proprietary Check Point "Reliable Data Protocol" (does not comply with RDP as specified in RFC 908/RFC 1151).	Connections to Security Gateway: • FWZ VPN (supported up to NG FP1 version only) • SecuRemote/SecureClient checks the availability of the Security Gateway/Desktop Policy Server • When more than one IP address is available on a Security Gateway for VPN, RDP probing method is used to determine which VPN link will be used between Check Point VPN Gateways (by VPND daemon)
UDP	260	*FW1_snmp* - Check Point Security Gateway SNMP Agent	Check Point's SNMP Agent listens on this port in addition to UDP port 161
TCP	261	*FW1_snauth* - Check Point Security Gateway Session Authentication	Communication between Security Gateway and Session Authentication API (SAA)
TCP	262	*not predefined*	*Loopback port* (used by MDQ process). Check Point Mail Dequeuer on SMTP Security Server.
TCP	264	*FW1_topo* - Check Point Security Gateway SecuRemote Topology Requests	Topology Download from Security Gateway (by FWD daemon) to SecuRemote (build 4100 and higher) and SecureClient
TCP	265	*FW1_key* - Check Point Security Gateway Public Key Transfer Protocol	• Exchanging CA-keys and DH-keys between management servers (SKIP, FWZ (4.x)) (by FWD daemon) • Public Key download from Security Gateway (by FWD daemon) to SecuRemote/SecureClient
TCP	301	*not predefined*	*Loopback port* (used by CVPND process). Back-end daemon of Mobile Access.
TCP	401	*not predefined*	*Loopback port* (used by PINGER process). Offload long-last requests from HTTPD process.
TCP	443	*not predefined*	Access to Management API
TCP	443	*not predefined*	• SmartView process on Security Management Server / Domain Management Server R80.x (sk111574) • SmartLog process on Security Management Server / Domain Management Server R80.x • Identity Awareness Agent connects on this port to Security gateway
TCP	443	*CP_SSL_Network_Extender* - SSL Network Extender port	• SSL Network Extender (SNX) • Remote Access Client configuration • Visitor Mode (by VPND daemon)
TCP	443	*not predefined*	Client -> Policy Server and Policy Server -> Endpoint Management Server communication (over HTTPS): Endpoint registration, new internal communication encryption key retrieval
TCP	443	*not predefined*	Client -> Policy Server and Policy Server -> Endpoint Management Server communication (encrypted ESP): FDE Recovery Data Upload, FDE User Acquisition & User Credentials, Media Encryption & Port Protection Key Exchange
TCP	443	*https* - HTTP protocol over TLS/SSL	Front-end daemon of Mobile Access (multi-processes - *mpdaemon*)
TCP	444		Required port for Remote Access client Site Creation
UDP	500	*IKE* - IPSEC Internet Key Exchange Protocol (formerly ISAKMP/Oakley)	IKE negotiation over UDP with Security Gateway (VPND daemon)
TCP	500	*IKE_tcp* - IPSEC Internet Key Exchange Protocol over TCP	IKE negotiation over TCP (by VPND daemon)
TCP	900	*FW1_clntauth_http* - Check Point Security Gateway Client Authentication (HTTP)	Client Authentication on Security Gateway (*in.ahclientd* daemon) using HTTP
TCP	981	*EDGE* - UTM-1 Edge Portal	Connection to UTM-1 Edge Web GUI when connecting via WAN port
TCP	1080	*not predefined*	Used by CPTNL client SOCKS proxy on Policy Server
TCP	1081	*not predefined*	Used by CPTNL client SOCKS proxy on Policy Server
TCP	1111	*IPSO_Clustering_Mgmt_Protocol* - Used for distributing configuration changes among cluster members and cluster wide monitoring	IPSO Clustering management connections to cluster members on IPSO OS
TCP	1129	*not predefined*	Synchronization between members of a Gaia Cloning Group
TCP	2010	*FIBMGR* - Forwarding Information Base Manager - Dynamic Routing Cluster configuration	FIB Manager connections from / to cluster members on SecurePlatform OS with enabled Dynamic Routing
TCP	2024	*not predefined*	Used internally on 61000/41000 Data Center Security Appliances for copying of SSM firmware file to SSM
UDP	2746	*VPN1_IPSEC_encapsulation* - Check Point Security Gateway SecuRemote IPSEC Transport Encapsulation Protocol	UDP encapsulation
TCP	4433	*CP_SmartPortal* - Check Point Smart Portal	Management Portal
TCP	4434	*not predefined*	Gaia Portal / SecurePlatform WebUI on Check Point Appliances
TCP	4500	*not predefined*	relevant for cases where TCP encapsulation is used fro RA VPN traffic
UDP	4500	*IKE_NAT_TRAVERSAL* - NAT Traversal (NAT-T) Protocol	NAT Traversal adds a UDP header, which encapsulates the IPSec ESP header (by VPND daemon).

TCP	4532	*not predefined*	*Loopback port* (used by IN.ASESSIOND process). Session Authentication.
UDP	5004	*MetaIP-UAT* - Check Point Meta IP UAM Client-Server Communication	IP address management (Note: Product is EOL)
TCP	5432	*PostgreSQL* - PostgreSQL database server	Move files between cluster members in order to perfrom DB synchronization (used by MOVEFILESERVER process)
TCP	6666	*not predefined*	Listened by FWM of Security Management Server / Customer Management Add-on (CMA) for communication arriving from CPM server.
TCP	6667	*not predefined*	Listened by FWM of the Multi-Domain Management Server for communication arriving from CPM server.
TCP	7087	*not predefined*	*Loopback port* (used by EMAILD / MSD / CTASD / CTIPD processes)
TCP	8005	*not predefined*	*Loopback port* (used by EPM process). Apache Tomcat server on Endpoint Security Management Server.
TCP	8009	*not predefined*	*Loopback port* (used by EPM process). Apache <--> Apache Tomcat AJP on Endpoint Security Management Server.
TCP	8080	*not predefined*	*Loopback port* (used by EPM process). Endpoint Security Management Server and Directory Scanner -> Apache Tomcat HTTP on Endpoint Security Management Server.
TCP	8080	*HTTP_and_HTTPS_proxy*	Front-end daemon of Mobile Access (used by multi-processes - *mpdaemon*)
TCP	8082	*not predefined*	Internal SmartView port
UDP	8116	*not predefined* - Cluster Control Protocol (CCP)	Communication between Check Point cluster members (Health Checks and State Synchronization)
TCP	8211	*not predefined*	• Connections between R80 Multi-Domain Security Management Server and Log Server • Used by SOLR - Logging core process
TCP	8443	*not predefined*	Used by Apache Tomcat HTTP on Endpoint Security Management Server
TCP	8880	*not predefined*	Security Gateway listens on this port for communication with Mobile Access.
TCP	8989	*not predefined*	*Loopback port* (used by CPD process). Used only on Provider-1 Customer Management Add-on (CMA) / Domain Management Server for Session Authentication - CAPS Messaging (*MSG_DEFAULT_PORT*).
TCP	9009	*not predefined*	Listened by CPM server for local connections (local SIC)
UDP	9281	*SWTP_Gateway* - VPN-1 Embedded/SofaWare commands	Connections (encrypted protocol) between Management Server (SMS daemon) and UTM-1 Edge devices
UDP	9282	*SWTP_SMS* - VPN-1 embedded / SofaWare Management Server (SMS)	Connections (encrypted protocol) between Management Server (SMS daemon) and UTM-1 Edge devices
TCP	9283	*not predefined*	SofaWare Management Server (SMS) Portal on Management Server
TCP	9876	*not predefined*	*Loopback port* (used by CVPNPROC process). Offload blocking commands from CVPND process (to prevent locks) - e.g., sending DynamicID.
UDP	9887	*cphamcset* - Clustering daemon	Responsible for opening sockets on the NICs to allow them to pass multicast traffic (CCP) to the machine.
TCP	9996	*not predefined*	Used by VPND daemon to synchronize session information (as a PostgreSQL) between VPND daemon and CVPND daemon (Mobile Access blade).
TCP	9998	*not predefined*	*Loopback port* (used by DBWRITER process). Offload DB commands from CVPND process (to prevent locks) and synchronize with other members.
TCP	10025	*not predefined*	Each e-mail is sent by Postfix to *in.emaild.mta* process to TCP port 10025
TCP	11680	*pepd* - Identity Awareness Captive Portal	The local port of the mini-Web server that does the redirection to the Captive Portal
TCP	12873	*cl_http_server* - Image server for Anti-Virus block page	Connections to Security Gateway to Image Server that sends images of the Anti-Virus block page returned to the user
TCP	15105	*identity_control_port* - Identity Control Blade	Connections from Identity Awareness PDP Gateway to Identity Awareness PEP Gateway - identity control sync to LDAP servers (AD controllers) and identity sharing in Identity Awareness
TCP	17000	*not predefined*	Identity Propagation from 3rd party identity providers (over SIC)
TCP	18181	*FW1_cvp* - Check Point OPSEC Content Vectoring Protocol	Connections (encrypted protocol) from Security Gateway to OPSEC Anti-Virus Server for Content Control
TCP	18181	*FW1_cvp*	Used by DLP Exchange Agent to send status information to Security gateway and/or Management.
TCP	18182	*FW1_ufp* - Check Point OPSEC URL Filtering Protocol	Connections (encrypted protocol) from Security Gateway to OPSEC URL Filtering Server for Content Control (e.g. Web Content)
TCP	18183	*FW1_sam* - Check Point OPSEC Suspicious Activity Monitor (SAM) API	• Connections from Management Server to FWD daemon on Security Gateway to instantly block suspicious connections (by FWD daemon) that are not restricted by the currently enforced security policy using the Suspicious Activity Rules feature in SmartView Monitor (Tools menu) • Connections from SmartEvent Server to FWD daemon on Management Server Monitor (*Tools* menu)
TCP	18183	*not predefined*	OPSEC Suspicious Activity Monitor (SAM) connections between GX / LTE SAM clients and Security Gateway (FWD daemon)
TCP	18184	*FW1_lea* - Check Point OPSEC Log Export API	Connections to Management Server (FWD daemon) for exporting FireWall logs using OPSEC Log Export API (LEA) products.
TCP	18185	*FW1_omi* - Check Point OPSEC Objects Management Interface	Protocol used by applications having access to the ruleset saved on Security Management Server
TCP	18186	*FW1_omi-sic* - Check Point OPSEC Objects Management Interface with Secure Internal Communication (SIC)	Secure Internal Communication (SIC) between OPSEC certified products and Security Gateway
TCP	18187	*FW1_ela* - Check Point OPSEC Event Logging API	Sending FireWall logs by OPSEC products (ELA) to Security Management Server (to FWD daemon)
TCP	18187	*FW1_ela*	Used by DLP Exchange Agent to send status information to Security gateway and/or Management.
TCP	18190	*CPMI* - Check Point Management Interface	Connections from GUI/SmartConsole clients / Management Portal / SmartReporter Server / SmartEvent Server to FWM daemon on Security Management Server / Multi-Domain Security Management Server / Domain Management Server.
TCP	18190	*not predefined*	SmartEndpoint / Endpoint Management Console -> Endpoint Security Management Server communication (over SIC)
TCP	18191	*CPD* - Check Point Daemon (CPD)	Connections to / from Management Server (CPD daemon): • Installing of rulebase from Security Management Server / Customer Management Add-on (CMA) / Domain Management Server to Security Gateway • Fetching rulebase by Security Gateway (during start) from Security Management Server / Customer Management Add-on (CMA) / Domain Management Server • Certificate revocation • "Test SIC Status" action
TCP	18192	*CPD_amon* - Check Point Internal Application Monitoring	Check Point internal Application Monitoring (AMON) connections between Security Gateway and Management Server / SmartReporter Server / SmartEvent Server (CPD daemon)
TCP	18193	*FW1_amon* - Check Point OPSEC Application Monitoring	Getting System Status from OPSEC products (by CPD daemon)
TCP	18193	*not predefined*	Endpoint Policy Server -> Endpoint Security Management Server communication (used by CPTNL server SOCKS proxy on Endpoint Policy Server)
TCP	18194	*not predefined*	• Connections from Security Gateway when running Threat Emulation as a remote emulator (by TED daemon) to Check Point Cloud • Connection from SandBlast agent to TE appliance when using remote Emulation (see sk116590)
TCP	18196	*not predefined*	Used to update the internal Application Monitoring (AMON) server (CPD daemon) on Endpoint Security Management Server with different status tables

TCP	18202	*CP_rtm* - Check Point Real Time Monitoring	Connections from Management Server to *Loopback port* (used by RTM process) for Real Time Monitoring (SmartView Monitor).
TCP	18205	*CP_reporting* - Check Point Reporting Client Protocol	Connections from SmartConsole clients (GUI) to Management Server (Reporting Server listens on this port).
TCP	18207	*FW1_pslogon* - Check Point Policy Server Logon protocol	Installing of Desktop Security policy from the Policy Server (DTPSD daemon) to SecureClient (4.x)
TCP	18208	*FW1_CPRID* - Check Point Remote Installation Protocol	Remote Installation of packages in SmartUpdate from Security Management Server / Customer Management Add-on (CMA) / Domain Management Server (by CPRID daemon) to Security Gateway
TCP	18209	*not predefined*	SIC communication (status, issue, revoke) between the Security Management Server (the Internal Certificate Authority (ICA)) and objects managed by this Security Management Sever (Security Gateways, OPSEC applications, etc.) (by FWM daemon)
TCP	18210	*FW1_ica_pull* - Check Point Internal CA Pull Certificate Service	Pulling certificates by Security Gateway from Security Management Sever (*ICA_PULL* , *FWCA_PULL_PORT*) (by CPCA daemon)
TCP	18211	*FW1_ica_push* - Check Point Internal CA Push Certificate Service	Pushing certificates from the Internal Certificate Authority (ICA) on Security Management Sever (by CPD daemon) to Security Gateway
UDP	18212	*FW1_load_agent* - Check Point ConnectControl Load Agent	Connections from Load Agent running on Load Balanced Servers (e.g., WWW, FTP) to Security Gateway
TCP	18221	*CP_redundant* - Check Point Redundant Management Protocol	Synchronization connections between Primary and Secondary Security Management Severs / Customer Management Add-ons (CMAs) / Domain Management Servers (by FWM daemon).
TCP	18221	*not predefined*	Endpoint Security Management Server <--> Secondary Endpoint Security Management Server communication (over SIC)
TCP	18231	*FW1_pslogon_NG* - Check Point NG Policy Server Logon protocol	Installing of Desktop Security policy from the Policy Server (DTPSD daemon) to SecureClient
TCP	18232	*FW1_sds_logon* - Check Point SecuRemote Distribution Server Protocol	Software distribution of Check Point components
UDP	18233	*FW1_scv_keep_alive* - Check Point SecureClient Verification Keepalive Protocol	Connections from SecureClient to Security Gateway for Secure Configuration Verification (SCV)
UDP	18234	*tunnel_test* - Check Point tunnel testing application	Check Point Tunnel Test packets from Security Gateway to test ICA through VPN with SecuRemote/SecureClient
UDP	18241	*E2ECP* - Check Point End to End Control Protocol	*Loopback port* (used by RTM process). Checking SLA's defined in Virtual Links by SmartView Monitor.
TCP	18262	*CP_Exnet_PK* - Check Point Extranet public key resolution	Exchange of public keys when configuring Extranet (not supported since NG AI R55)
TCP	18263	*CP_Exnet_resolve* - Check Point Extranet remote objects resolution	Importing exported objects from partner in Extranet (not supported since NG AI R55)
TCP	18264	*FW1_ica_services* - Check Point Internal CA Fetch CRL and User Registration Services	Connections to Management Server for Certificate Revocation Lists (CRLs) and registering users when using the Policy Server. Refer to sk35292.
TCP	18265	*FW1_ica_mgmt_tools* - Check Point Internal CA Management Tools	Internal CA Management (ICA) connections from SmartConsole GUI client hosts to Management Server
TCP	18266	*CP_seam* - Check Point Eventia Analyzer Server Protocol	Connections to Eventia Analyzer Server / SmartEvent Server.
TCP	18272	*not predefined*	Used by PostgreSQL on Endpoint Management Server
TCP	18300	*UserCheck* - Check Point Daemon Protocol	UserCheck connections from internal hosts to DLP Gateway (USRCHKD daemon) - policy-driven user interaction for Application Control, URL Filtering, DLP
TCP	18301	*CheckPointExchangeAgent*	Connections (in clear) from Exchange Agent (running on Microsoft Exchange Server) to DLP Gateway
TCP	19009	*CPM* - Check Point Management Server	Listened by CPM server for remote connections (For example SmartConsole. Added in R80)
TCP	19190	*FW1_netso* - Check Point User Authority simple protocol	Communication from UserAuthority Server to Web Plugin when authenticating using certificates generated by the Internal Certificate Authority (ICA)
TCP	19191	*FW1_uaa* - Check Point OPSEC User Authority API	Connections from Security Gateways / Hosts with User Authority products to UserAuthority Server
UDP	19194 and 19195	*CP_SecureAgent-udp* - User Authority SecureAgent Authentication service	User Authority SecureAgent Authentication ICA service
TCP	20000	*not predefined*	Used internally on 61000/41000 Data Center Security Appliances on the SSM during the firmware upgrade
TCP	28581	*identity_control_port* - Identity Awareness	Connections from Identity Awareness PEP Gateway to Identity Awareness PDP Gateway - sharing of identities between gateways
TCP	30580	*not predefined*	*Loopback port* (used by TED process). Communication with files sent via the DLPU process.
TCP	31415	*not predefined*	For Primary Endpoint Management Server <--> Secondary Endpoint Management Server and Endpoint Management Server <--> Web Remote Help server communications only when synchronization method is automatic online (starting from R77.20)
TCP	60706	*not predefined*	*Loopback port* (used by CPWMD process). The back-end for web user interface on SecurePlatform OS (Check Point Web Management).
TCP	60709	*not predefined*	*Loopback port* (used by CPWMD process). The back-end for web user interface on Gaia OS (Check Point Web Management).
TCP	61616	*not predefined*	*Loopback port* (used by EPM process). Apache ActiveMQ (AMQ) access on Endpoint Security Management Server.
TCP	65524	*FW1_sds_logon_NG* - SecuRemote Distribution Server Protocol (VC and higher)	Software distribution of Check Point components in NG versions
IP 17	---	*tunnel_test_mapped* - Tunnel testing for a module performing the tunnel test	VPN tunnel testing for a module performing the tunnel test
IP 50	---	*ESP* - IPSEC Encapsulating Security Payload Protocol	Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite. In IPsec it provides origin authenticity, integrity and confidentiality protection of packets.
IP 94	---	*FW1_Encapsulation* - Check Point Security Gateway SecuRemote FWZ Encapsulation Protocol	Encryption scheme for SecuRemote
IP 112	---	*vrrp* - Virtual Router Redundancy Protocol	VRRP connections to IP 224.0.0.18, Proto 112, TTL 255