Web Security Default Ports

Topic 50099 | Web Security Default Ports | Web Security Solutions | Updated 06-May-2013

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

This reference identifies the default ports used by Websense Web Security Gateway components, including interoperability components used to communicate with Websense Data Security and, in Websense Web Security Gateway Anywhere deployments, the hybrid service.

In most cases, the default ports, which are assigned automatically during installation, never need to be changed. If you do need to change a port:

- (*Versions 7.5 and 7.6*) Use the Log Server Configuration utility to change the Log Server port.
- (*Version 7.7*) Use the Settings > Reporting > Log Server page in TRITON - Web Security to change the Log Server port.
- (*All versions*) Use TRITON - Web Security to configure communication with Log Server if the port has changed, and to change port information for transparent identification agents (DC Agent, eDirectory Agent, Logon Agent, or RADIUS Agent).

If you need to change ports for other services, this can be done in the initialization (INI) file for the component. Given dependencies between components, the change may need to be made in multiple files. If instructions for the component that you need to reconfigure are not available, contact Websense Technical Support for assistance. Instructions for changing the Policy Server and Policy Broker ports can be found in the Server Administration section of the TRITON - Web Security Help (version 7.5, version 7.6, and version 7.7).

A diagram that provides an overview of component connections and communications ports, as well as an Excel spreadsheet of the port list, are also available for version 7.7.

Control Service ports

Topic 50115 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Control Service manages installation, configuration, addition, and removal of Websense Web Security components. It is installed automatically on all Websense software machines, and should not be disabled or removed independently of other Websense components.

Port	Description
55933	Web service port
55939	Clustering port

Policy Broker ports

Topic 50103 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Policy Broker manages requests from Websense components for policy and general configuration information, stored in the Policy Database.

Port	Direction	Protocol	Description
6432 7432		TCP	Policy Database connection (local to the Policy Broker machine; does not need to be opened on firewalls)
55880	Inbound	TCP	Used for communication with Policy Server, Filtering Service, Log Server, Usage Monitor, and TRITON - Web Security

Policy Server ports

Topic 50104 | Web Security Default Ports | Web Security Solutions | Updated 18-Jun-2013

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Policy Server identifies and tracks the location and status of other Websense Web Security components, and:

- Stores configuration information specific to a single Policy Server instance.
- Communicates configuration data to Filtering Service, for use in filtering Internet requests.

Port	Direction	Protocol	Description
25	Outbound	TCP	SMTP port
162	Outbound	TCP	SNMP port
40000	Inbound	TCP	Negotiate encryption port
55806	Inbound	TCP	Configuration information exchange port
55807	Outbound	TCP	Filtering Service
55808	Outbound	TCP	Integration Service
55811	Outbound	TCP	Network Agent
55812	Outbound	TCP	Log Server
55813	Outbound	TCP	Usage Monitor
55815	Outbound	TCP	User Service
55817	Outbound	TCP	Explorer Scheduler
55818	Outbound	TCP	Explorer Information Service
55819	Outbound	TCP	Logon Agent
55821	Outbound	TCP	eDirectory Agent
55822	Outbound	TCP	RADIUS Agent
55823	Outbound	TCP	DC Agent
55824	Outbound	TCP	TRITON - Web Security
55826	Outbound	TCP	Content Gateway
55827	Outbound	TCP	Download Server
55810	Inbound	TCP	Diagnostics
55830	Outbound	TCP	Sync Service
55880	Outbound	TCP	Policy Broker
55900	Outbound	TCP	Directory Agent
55905		UDP	UID broadcast
Indeterminate	Outbound	TCP	(*v7.7*) Websense Multiplexer

Filtering Service ports

Topic 50105 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Filtering Service provides Internet filtering in conjunction Network Agent, Content Gateway, or a third-party integration product. When a user requests a site, Filtering Service receives the request and determines which policy applies.

- Filtering Service must be running for Internet requests to be filtered and logged.
- All Filtering Service machines must have Internet access, because each instance downloads its own copy of the Websense Master Database.

Port	Direction	Protocol	Description
80	Outbound	TCP	Master Database download server
15868	Inbound	TCP	WISP: Network Agent, Remote Filtering Server, Linking Service, filtering plug-ins (ISAPI and Citrix), integrations
15869		UDP	Diagnostics
15871	Inbound	TCP	Block pages (browser requests the page from the Filtering Service block page server)
30600	Outbound	TCP	DC Agent
30602	Outbound	TCP	Logon Agent
30700	Outbound	TCP	eDirectory Agent
30800	Outbound	TCP	RADIUS Agent
40000	Outbound	TCP	Policy Server (negotiate encryption)
55805	Outbound	TCP	Log Server
55806	Outbound	TCP	Policy Server (configuration exchange)
55807	Inbound	TCP	Listening port (WIFFLE): Policy Server, TRITON - Web Security toolbox
55808		TCP	(*v7.5 and v7.6*) Integration Service
55809	Outbound	TCP	Usage Monitor
55815	Outbound	TCP	User Service
55828	Outbound	TCP	(*v7.7*) State Server (track state information for Quota, Continue, Password Override, and other time-based filtering options in multiple Filtering Service environments)
55833	Outbound	TCP	Multiplexer (when SIEM integration is enabled)
55880	Outbound	TCP	Policy Broker

User Service ports

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

User Service communicates with the directory service to convey user-related information, including user-to-group and user-to-domain relationships, to Policy Server and Filtering Service for use in applying filtering policies.

If you have installed and configured a Websense transparent identification agent, User Service helps to interpret user logon session information, and uses this information to provide user name-to-IP-address associations to Filtering Service.

When you add users and groups as clients, User Service provides name and path information from the directory service to TRITON - Web Security.

Port	Direction	Protocol	Description
139	Outbound	TCP	NetBIOS communication: Active Directory
389	Outbound	TCP	LDAP communication: Active Directory, Novell eDirectory, Sun Java System
636	Outbound	TCP	SSL port: Novell eDirectory, Sun Java System
3268	Outbound	TCP	Active Directory
3269	Outbound	TCP	SSL port: Active Directory
15872	Inbound	TCP	Secure manual authentication
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Server (configuration exchange)
55815	Inbound	TCP	Listening port (WIFFLE): Filtering Service, Linking Service, Reporting, TRITON - Web Security
55840		UDP	Diagnostics
55880	Outbound	TCP	Policy Broker

Log Server ports

Topic 50107 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Log Server logs Internet request data, including:

- The request source
- The category or protocol associated with the request
- Whether the request was permitted or blocked
- Whether keyword blocking, file type blocking, quota allocations, bandwidth levels, or password protection were applied

With Network Agent and some integration products, Log Server also stores information about the amount of bandwidth used.

Log Server is a Windows-only component that must be installed to enable all reporting features of TRITON - Web Security.

Port	Direction	Protocol	Description
1433	Outbound	TCP	SQL Server communication (ODBC port)
40000	Outbound	TCP	Policy Server (negotiate encryption)
55805	Inbound	TCP	Logging port
55806	Outbound	TCP	Policy Server (configuration exchange)
55812	Inbound	TCP	Policy Broker callback; Content Gateway logs
55815	Outbound	TCP	User Service
55880	Outbound	TCP	Policy Broker
55885	Inbound	TCP	Sync Service (hybrid log records)

Network Agent ports

Topic 50108 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Network Agent enables filtering in a standalone environment. It also:

- Enhances filtering and logging functions
- Enables protocol management for non-HTTP protocols

Port	Direction	Protocol	Description
15868	Outbound	TCP	Filtering Service
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Sever (configuration exchange)
55811	Inbound	TCP	Listening (WIFFLE)
55870		UDP	Diagnostics
55880	Outbound	TCP	Policy Broker

Usage Monitor ports

Topic 50109 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Usage Monitor enables alerting based on Internet usage. It tracks access to categories and protocols, and generates alert messages according to the alerting behavior you have configured.

Port	Direction	Protocol	Description
25	Outbound	TCP	Email alerts
162	Outbound	TCP	SNMP alerts
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Sever (configuration exchange)
55809	Inbound	TCP	Filtering Service
55813	Inbound	TCP	Policy Server
55816		UDP	Diagnostics
55835	Outbound	TCP	Real-Time Monitor
55880	Outbound	TCP	Policy Broker

TRITON - Web Security ports

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

TRITON - Web Security is the TRITON console module that serves as the configuration, management, and reporting interface for Websense Web Security.

Use TRITON - Web Security to define and customize Internet access policies, configure security components, report on Internet activity, and more.

Port	Direction	Protocol	Description
1433		TCP	SQL Server (ODBC), used to connect to the Log Database
1822		TCP	Apache HTTP Server uses this port for HTTP communication.
7191		TCP	Apache Tomcat uses this port for HTTP communication.
7443		TCP	(*v7.5*) Linking port (for connection to TRITON - Data Security)
8080		TCP	Management console communication with administrator browsers
9009		TCP	AJP: Apache Tomcat uses this port to communicate with Apache HTTP Server.
9443		TCP	Tomcat (management) port, used when administrators connect to the TRITON console
9444		TCP	Apache (reporting)
9445		TCP	HTTPS communication between the TRITON console and RTM Client
18445	Inbound	TCP	(*v7.7*) Content Gateway, used to register with the forensics repository. Limit the port to allow connections only from Content Gateway machines.
40000	Outbound	TCP	Policy Server (negotiate encryption)
55805	Outbound	TCP	Log Server
55806	Outbound	TCP	Policy Sever (configuration exchange)
55807	Outbound	TCP	Filtering Service
55815	Outbound	TCP	User Service
55817	Outbound	TCP	Explorer Scheduler
55818	Outbound	TCP	Explorer Information Service
55824	Inbound	TCP	Listening port (WIFFLE)
55880	Outbound	TCP	Policy Broker

Real-Time Monitor ports

Topic 50121 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7

Real-Time Monitor provides insight into current Internet filtering activity in your network, showing the URLs being requested and the action applied to each request.

Real-Time Monitor includes 3 services: RTM Server, RTM Client, and RTM Server, all installed on the same machine.

Port	Direction	Protocol	Description
9092		TCP	RTM Server and Client communication with RTM Database (only used for components on the same machine)
9445		TCP	HTTPS communication between the TRITON console and RTM Client
55809	Outbound	TCP	Usage Monitor listening port
55835	Inbound	TCP	RTM Server listening port (receives data from Usage Monitor)
55836*	Outbound	TCP	Policy Server (WIFFLE communication)
55856*	Outbound	TCP	Policy Server (secure WIFFLE communication)

* Note that when connecting to Policy Server, RTM Server can use any port in a 20-port range. The default port is shown above. If that port is in use, RTM Server increments the port number by 1 and tries again, until it either finds a free port or reaches the end of the range.

State Server ports

Topic 50122 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7

In multiple Filtering Service deployments, State Server tracks session information to enable the use of time-based filtering actions, like Quota, Continue, Password Override, and Account Override.

Deploy only one State Server instance per logical deployment, or group of Filtering Service instances that might handle requests from the same set of users. A geographically distributed organization might have one State Server for their 5 Filtering Service instances in the Eastern U.S., another for their 3 Filtering Service instances in Sidney, Australia, and a third for their 3 Filtering Service instances in Cape Town, South Africa.

Port	Direction	Protocol	Description
55828	Inbound		Filtering Service communication

Linking Service ports

Topic 50111 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

In Websense Web Security Gateway Anywhere deployments, or in environments that combine Websense data and Web security solutions, Linking Service:

- Gives data security software access to Master Database categorization information
- Gives data security software access to user and group information collected by User Service
- Enables shared administrative access to the Web Security and Data Security modules of the TRITON Unified Security Center

Port	Direction	Protocol	Description
7443		TCP	(*Version 7.5*) Linking port, used to connect TRITON - Web Security and TRITON - Data Security
15868	Outbound	TCP	Filtering Service (Master Database information)
56992	Outbound	TCP	Used to communicate URL category and user information to Data Security components.
55815	Outbound	TCP	User Service

Multiplexer ports

Topic 50123 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7

Websense Multiplexer simplifies the process of integrating Websense Web Security solutions with a third-party SIEM integration. When SIEM integration is activated, Internet activity data collected by Filtering Service is passed by the Multiplexer to both the SIEM product and Websense Log Server. (When no SIEM integration is used, Filtering Service passes Internet activity data to Log Server directly.)

Port	Direction	Port	Description
514	Outbound	TCP	SIEM integration (default TCP port)
515	Outbound	UDP	SIEM integration (default UDP port)
40000	Outbound	TCP	Policy Server (negotiate encryption)
55805	Outbound	TCP	Log Server (log data)
55806	Outbound	TCP	Policy Sever (configuration exchange)
55833	Inbound	TCP	Filtering Service (log data)
56011		UDP	Diagnostics
			Multiplexer uses an indeterminate port as its WIFFLE listening port.

Sync Service ports

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

In Websense Web Security Gateway Anywhere deployments, Sync Service:

- Sends policy updates and user and group information to the hybrid service.
- Receives reporting data from the hybrid service.

Only one Sync Service instance is permitted per deployment. Sync Service is typically installed on the Log Server machine.

Port	Direction	Protocol	Description
443	Outbound	TCP	Hybrid filtering
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Server (configuration exchange)
55830	Inbound	TCP	Listening (WIFFLE)
55831	Outbound	TCP	Policy Server secure communication
55832	Outbound	TCP	Directory Agent, Tomcat (HTTP connection)
55880	Outbound	TCP	Policy Broker
55885	Outbound	TCP	Log Server

Note that Websense Web Security Gateway Anywhere deployments, client machines filtered by the hybrid service must be configured to allow connections on port **80** from one of the following in order for hybrid block messages to be displayed:

- (v7.5, v7.6, or v7.7) **hybrid-web.global.blackspider.com:8081**
- (v7.7) **hybrid-web.global.blackspider.com:8082**

Directory Agent ports

Topic 50113 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

In Websense Web Security Gateway Anywhere deployments, Directory Agent collects user and group information from a supported directory service (Windows Active Directory [Native Mode] or Novell eDirectory) for use in filtering by the hybrid service.

Directory Agent must be able to communicate with both the directory and Sync Service for user and group data to be available for hybrid filtering.

Port	Direction	Port	Description
389	Outbound	TCP	Active Directory, Novell eDirectory
3268	Outbound	TCP	Active Directory
3269	Outbound	TCP	SSL: Active Directory
686	Outbound	TCP	SSL: Novell eDirectory
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Server (configuration exchange)
55832	Inbound	TCP	Sync Service
55900	Inbound	TCP	Listening (WIFFLE)

Note that in Websense Web Security Gateway Anywhere deployments, client machines filtered by the hybrid service must be configured to allow connections from **hybrid-web.global.blackspider.com:8081** on port **80** in order for hybrid block messages to be displayed.

Remote Filtering Server ports

Topic 50114 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Remote Filtering Server allows filtering of clients outside a network firewall. It communicates with Filtering Service in the local network and the Remote Filtering Client on the remote machine to provide Internet access management for users who are off-site.

Port	Direction	Protocol	Description
80 8080	Inbound	TCP	Remote Filtering Client (proxy port)
8800	Inbound	TCP	Remote Filtering Client (heartbeat port)
15868	Outbound	TCP	Filtering Service
15871	Outbound	TCP	Filtering Service (request block pages)
40000	Outbound	TCP	Installation only: Policy Server (negotiate encryption)
55806	Outbound	TCP	Installation only: Policy Server (configuration exchange)
55880	Outbound	TCP	Policy Broker

DC Agent ports

Topic 50116 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

DC Agent offers transparent user identification for users defined in a Windows-based directory, and communicates with User Service to provide up-to-date user logon session information to Websense software for use in filtering.

Port	Direction	Protocol	Description
137 138 139 445	Outbound	TCP	NetBIOS: domain controller (Active Directory)
30600	Inbound	TCP	Filtering Service
30601		UDP	Diagnostics
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Server (configuration exchange)
55823	Inbound	TCP	Listening (WIFFLE)

Logon Agent ports

Topic 50117 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Logon Agent provides unsurpassed accuracy in transparent user identification in Linux and Windows networks. The agent:

- Does not rely on a directory service or other intermediary when capturing user logon sessions
- Detects user logon sessions as they occur

Logon Agent communicates with the logon application to ensure that individual user logon sessions are captured and processed directly by Websense software.

Port	Direction	Protocol	Description
15880	Outbound	TCP	Logon application
30602	Inbound	TCP	Filtering Service
30603		UDP	Diagnostics
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Server (configuration exchange)
55819	Outbound	TCP	Listening (WIFFLE)

eDirectory Agent ports

Topic 50118 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

eDirectory Agent works with Novell eDirectory to transparently identify users. The agent:

- Gathers user logon session information from Novell eDirectory, which authenticates users logging on to the network.
- Associates each authenticated user with an IP address, and then works with User Service to supply the information to Filtering Service.

Port	Direction	Protocol	Description
389	Outbound	TCP	Novell eDirectory
686	Outbound	TCP	SSL: Novell eDirectory
30700	Inbound	TCP	Filtering Service
30701		UDP	Diagnostics
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Server (configuration exchange)

RADIUS Agent ports

Topic 50119 | Web Security Default Ports | Web Security Solutions | Updated 28-Sep-2012

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

RADIUS Agent enables transparent identification of users who use a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection to access the network.

Ports	Direction	Protocol	Description
1645		TCP	RADIUS server (authentication)
1646		TCP	RADIUS server (account)
12345		TCP	RAS/VPN (authentication)
12346		TCP	RAS/VPN (account)
30800	Inbound	TCP	Filtering Service, RADIUS client
30801		UDP	Diagnostics
40000	Outbound	TCP	Policy Server (negotiate encryption)
55806	Outbound	TCP	Policy Server (configuration exchange)
55822	Inbound	TCP	Listening (WIFFLE)

Content Gateway ports

Topic 50120 | Web Security Default Ports | Web Security Solutions | Updated 18-Jun-2013

Applies to:	Web Security Gateway and Web Security Gateway Anywhere, v7.5, 7.6, 7.7

Content Gateway provides Websense Web Security with the advantages of a proxy cache, improving bandwidth usage and network performance by storing requested Web pages and, while a stored page is considered fresh, serving that Web page to the requesting client.

Content Gateway ports v7.7

> **Note**
> Inbound ports that also connect outbound to the internet are notated by an asterisk (*).

Ports	Direction	Protocol	Description
*21	Inbound	TCP	Transparent proxy FTP traffic
22	Inbound	TCP	SSH port, used for command-line access
53 5353	Inbound	UDP	Used for DNS communication
*80	Inbound	TCP	Transparent proxy HTTP traffic
88	Outbound	TCP/UDP	Kerberos
389	Outbound	TCP/UDP	LDAP
*443	Inbound	TCP	Transparent proxy HTTPS traffic
445	Outbound	TCP	IWA &NTLM
1080	Inbound	TCP	SOCKS
1812	Outbound	UDP	RADIUS
2048	Inbound	UDP	Transparent proxy using WCCP
2121	Inbound	TCP	Explicit proxy FTP traffic
3130	Inbound	UDP	Internet Cache Protocol (ICP) port used to enable a cache hierarchy.
8070	Inbound	TCP	Reserved by Content Gateway for Transparent Proxy HTTPS traffic
8071	Inbound	TCP	Content Gateway Manager SSL port
8080	Inbound	TCP	Explicit proxy HTTP and HTTPS traffic
8081	Inbound	TCP	Content Gateway Manager HTTP port

Ports	Direction	Protocol	Description
8089	Inbound	UDP	SNMP encapsulation
9447	Outbound	TCP	Appliance Manager administrator access
15868	Inbound	TCP	Filtering Service communication (WISP)
40000	Inbound	TCP	Policy Server (negotiate encryption)
55806	Inbound	TCP	Policy Server (configuration exchange)
55826	Inbound	TCP	Policy Server (callback)
55829	Inbound	TCP	WTG app
55880	Inbound	TCP	Policy Broker (policy information exchange)
55905	Inbound	UDP	UID broadcast

Clustering

Content Gateway uses a proprietary protocol for clustering, which is multicast for node discovery and heartbeat, but unicast for all data exchange within the cluster. The following ports are used.

Ports	Direction	Description
8082	Inbound	Clustering statistics gathering
8083	Inbound	Autoconfiguration for clustering (PAC file)
8084	Inbound	Process manager for clustering
8085	Inbound	Logging server for clustering
8086	Inbound	Enables clustering
8087	Inbound	Reliable service for clustering
8088	Inbound	Multicast for clustering

Data Security communication

In Websense Web Security Gateway Anywhere deployments, or other deployments that combine Websense Web Security and Data Security components, Content Gateway uses the following ports for integration and communication with Data Security:

Ports	Direction	Protocol	Description
17500	Inbound + Outbound	TCP	Date Security configuration
17501	Inbound + Outbound	TCP	Reserved for Data Security configuration
17502	Inbound + Outbound	TCP	Reserved for Data Security configuration
17503	Inbound + Outbound	TCP	Data Security remote analysis
17504	Inbound + Outbound	TCP	Reserved for Data Security remote analysis

17505	Inbound + Outbound	TCP	Data Security fingerprint detection
17506	Inbound + Outbound	TCP	Reserved for Data Security fingerprint detection
17507	Inbound + Outbound	TCP	Reserved for Data Security configuration
17508	Inbound + Outbound	TCP	Reserved for Data Security configuration
17509	Inbound + Outbound	TCP	Reserved for Data Security configuration
17510	Inbound + Outbound	TCP	Reserved for Data Security
17511	Inbound + Outbound	TCP	Reserved for Data Security
17512	Inbound + Outbound	TCP	Data Security OCR
17513	Inbound + Outbound	TCP	Reserved for Data Security remote analysis
17514	Inbound + Outbound	TCP	Reserved for Data Security

Content Gateway ports v7.5, 7.6

Ports	Protocol	Description
21	TCP	Transparent proxy FTP traffic
22	TCP	SSH port, used for command-line access
53 5353	UDP	Used for DNS communication
80	TCP	Transparent proxy HTTP traffic
443	TCP	Transparent proxy HTTPS traffic
2048	UDP	Transparent proxy using WCCP
2121	TCP	Explicit proxy FTP traffic
3130	UDP	Internet Cache Protocol (ICP) port used to enable a cache hierarchy.
8070	TCP	(Version 7.5 only) Explicit proxy HTTPS traffic
8071	TCP	Content Gateway Manager SSL port
8080	TCP	(v7.5) Explicit proxy HTTP traffic (v7.6) Explicit proxy HTTP and HTTPS traffic
8081	TCP	Content Gateway Manager HTTP port
8089	UDP	SNMP encapsulation
8090	TCP	HTTPS outbound (between Content Gateway and the SSL outbound proxy)
9447	TCP	Appliance Manager administrator access
15868	TCP	Filtering Service communication (WISP)

Ports	Protocol	Description
30900	TCP	Download service
40000	TCP	Policy Server (negotiate encryption)
55806	TCP	Policy Server (configuration exchange)
55880	TCP	Policy Broker (policy information exchange)
55905	UDP	UID broadcast
Random (1024 - 65535)	TCP	(*Version 7.5*) Establish communication with off-box Policy Server

Clustering

Content Gateway uses a proprietary protocol for clustering, which is multicast for node discovery and heartbeat, but unicast for all data exchange within the cluster. The following ports are used.

Ports	Description
8082	Clustering statistics gathering
8083	Autoconfiguration for clustering (PAC file)
8084	Process manager for clustering
8085	Logging server for clustering
8086	Enables clustering
8087	Reliable service for clustering
8088	Multicast for clustering

Data Security communication

In Websense Web Security Gateway Anywhere deployments, or other deployments that combine Websense Web Security and Data Security components, Content Gateway uses the following ports for integration and communication with Data Security:

Ports	Protocol	Description
5819	TCP	Data Security fingerprint detection
5820	TCP	Data Security fingerprint synchronization
5821 5822 5823	TCP	Data Security fingerprint configuration
8880	TCP	Data Security configuration
8888 8889	TCP	Data Security deployment and system health information
8892	TCP	Data Security system logging
9080 9081	TCP	Data Security statistics and system health information

9090 9091	TCP	Data Security diagnostics
18303	TCP	Data Security local analysis
18404	TCP	Data Security remote analysis