IP Interfaces and Accessing the Appliance

This chapter contains the following sections:

- IP Interfaces and Accessing the Appliance, on page 1
- IP Interfaces, on page 1

IP Interfaces and Accessing the Appliance

You can access any IP interface you create on a Cisco Content Security appliance through a variety of services.

By default, the following services are either enabled or disabled on each interface:

Table 1: Services Enabled by Default on IP Interfaces

		Enabled by default?	
Service	**Default Port**	**Management Interface**	**New IP Interfaces You Create**
FTP	21	No	No
Telnet	23	Yes	No
SSH	22	Yes	No
HTTP	80	Yes	No
HTTPS	443	Yes	No

IP Interfaces

An IP interface contains the network configuration data needed for an individual connection to the network. You can configure multiple IP interfaces to a physical Ethernet interface. You can also configure access to the spam quarantine via an IP interface. For email delivery and Virtual Gateways, each IP interface acts as one Virtual Gateway address with a specific IP address and hostname. You can also “join” interfaces into distinct groups (via the CLI), and the system will cycle through these groups when delivering email. Joining or grouping Virtual Gateways is useful for load-balancing large email campaigns across several interfaces. You can also create VLANs, and configure them just as you would any other interface (via the CLI). For more

information, see the “Advanced Networking” chapter in the user guide or online help for your Email Security appliance.

Configuring IP Interfaces

The Management Appliance > Network > IP Interfaces page (and interface config command) enables you to add, edit, or delete IP interfaces.

Note You cannot change the name or Ethernet port associated with the Management interface on the Security Management appliance. Further, the Security Management appliance does not support all of the features discussed below (Virtual Gateways, for example).

The following information is required when you configure an IP interface:

Table 2: IP Interface Components

Name	**The nickname of the interface.**
IP address	IP addresses within the same subnet cannot be configured on separate physical Ethernet interfaces.
Netmask (or subnetmask)	You can enter the netmask in standard dotted octet form (for example, 255.255.255.0) or hexadecimal form (for example, 0xffffff00). The default netmask is 255.255.255.0, a common class C value.
Broadcast address	AsyncOS automatically calculates the default broadcast address from the IP address and the netmask.
Hostname	The hostname that is related to the interface. This hostname is used to identify the server during the SMTP conversation. You are responsible for entering a valid hostname associated with each IP address. The software does not check that DNS correctly resolves the hostname to the matching IP address, or that reverse DNS resolves to the given hostname.
Allowed services	FTP, SSH, Telnet, spam quarantine, HTTP, and HTTPS can be enabled or disabled on the interface. You can configure the port for each service. You can also specify the HTTP/HTTPS, port, and URL for the spam quarantine.

Note If you have completed the System Setup Wizard as described in Setup, Installation, and Basic Configuration and committed the changes, the Management interface should already be configured on the appliance.

Creating IP Interfaces Using the GUI

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > Network > IP Interfaces**.

Step 3 Click **Add IP Interface**.

Step 4 Enter a name for the interface.

Step 5 Select an Ethernet port and enter an IP address.

Step 6 Enter the netmask for the IP address.

Step 7 Enter a hostname for the interface.

Step 8 Select the check box next to each service you want to enable on this IP interface. Change the corresponding port if necessary.

Step 9 Select whether to enable redirecting HTTP to HTTPS for appliance management on the interface.

Step 10 If you are using the spam quarantine, you can select HTTP or HTTPS or both and specify the port numbers for each. You can also select whether to redirect HTTP requests to HTTPS. Finally, you can specify whether the IP interface is the default interface for the spam quarantine, and whether to use the hostname as the URL or provide a custom URL.

Step 11 Submit and commit your changes.

Accessing the Appliance via FTP

Caution By disabling services via the Management Appliance > Network > IP Interfaces page or the interfaceconfig command, you can disconnect yourself from the GUI or CLI, depending on how you are connected to the appliance. Do not disable services with this command if you are not able to reconnect to the appliance using another protocol, the Serial interface, or the default settings on the Management port.

Step 1 [New Web Interface Only] On the Security Management appliance, click to load the legacy web interface.

Step 2 Choose **Management Appliance** > **Network** > **IP Interfaces** page (or the `interfaceconfig` command) to enable FTP access for the interface.

Note Remember to commit your changes before moving on to the next step.

Step 3 Access the interface via FTP. Ensure you are using the correct IP address for the interface.

Example: `ftp 192.168.42.42`

Many browsers also allow you to access interfaces via FTP.

Example: `ftp://192.10.10.10`

Step 4 Browse to the directory for the specific task you are trying to accomplish. After you have accessed an interface via FTP, you can browse the following directories to copy and add ("`GET`" and "`PUT`") files. See the following table.

Table 3: Directories Available for Access

Directory Name	Description
/avarchive /bounces /cli_logs /delivery /error_logs /ftpd_logs /gui_logs /mail_logs /rptd_logs /sntpd.logs /status /system_logs	Created automatically for logging via the Management Appliance > System Administration > Log Subscriptions page or the logconfig and rollovernow commands. See the "Logging" chapter in the user guide or online help for your Email Security appliance for a detailed description of each log. See "Log File Type Comparison" in the "Logging" chapter for the differences among each log file type.
/configuration	The directory where data from the following pages and commands are exported to and/or imported (saved) from: • Virtual Gateway mappings (altsrchost) • Configuration data in XML format (saveconfig, loadconfig) • Host Access Table (HAT) page (hostaccess) • Recipient Access Table (RAT) page (rcptaccess) • SMTP Routes page (smtproutes) • Alias tables (aliasconfig) • Masquerading tables (masquerade) • Message filters (filters) • Global unsubscribe data (unsubscribe) • Test messages for the trace command
/MFM	The Mail Flow Monitoring database directory contains data for the Mail Flow Monitor functionality available from the GUI. Each subdirectory contains a README file that documents the record format for each file. You can copy these files to a different machine for record keeping, or load the files into a database and create your own analysis application. The record format is the same for all files in all directories; this format may change in future releases.
/periodic_reports	The directory where all archived reports configured on the system are stored.

Step 5 Use your FTP program to upload and download files to and from the appropriate directory.

Secure Copy (scp) Access

If your client operating system supports a secure copy (`scp`) command, you can copy files to and from the directories listed in the table *Directories Available for Access*. For example, in the following example, the file /tmp/test.txt is copied from the client machine to the configuration directory of the appliance with the hostname mail3.example.com .

Note The command prompts for the user's passphrase (admin). This example is shown for reference only; your operating system's implementation of secure copy may vary.

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.
admin@mail3.example.com's passphrase: (type the passphrase)
test.txt             100% |***************************|  1007       00:00
%
```

In this example, the same file is copied from the appliance to the client machine:

```
% scp admin@mail3.example.com:configuration/text.txt .
admin@mail3.example.com's passphrase: (type the passphrase)
test.txt             100% |***************************|  1007       00:00
```

You can use secure copy (scp) as an alternative to FTP to transfer files to and from the content security appliance.

Note Only users in the operators and administrators group can use secure copy (scp) to access the appliance. For more information, see About Reverting to an Earlier Version of AsyncOS.

Accessing via a Serial Connection

If you are connecting to the appliance via a serial connection, use the following information for the console port.

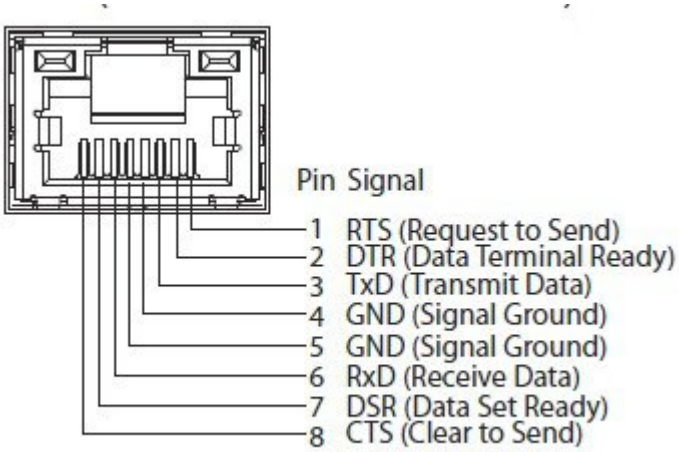
Complete information about this port is in the hardware installation guide for your appliance.

Related Topics

- Documentation

Pinout Details for the Serial Port in 80- and 90- Series Hardware

Figure 1: Pinout Details for the Serial Port in 80- and 90- Series Hardware



Pinout Details for the Serial Port in 70-Series Hardware

The following figure illustrates the pin numbers for the serial port connector, and the table *Serial Port Pin Assignments* defines the pin assignments and interface signals for the serial port connector.

Figure 2: Pin Numbers for the Serial Port

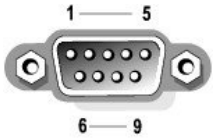


Table 4: Serial Port Pin Assignments

Pin	Signal	I/O	Definition
1	DCD		Data carrier detect
2	SIN		Serial input
3	SOUT		Serial output
4	DTR		Data terminal ready
5	GND	n/a	Signal ground
6	DSR		Data set ready
7	RTS		Request to send
8	CTS		Clear to send

Pin	Signal	I/O	Definition
9	RI		Ring indicator
Shell	n/a	n/a	Chassis ground

IP Interfaces and Accessing the Appliance