FTP, SSH, and SCP Access

This appendix contains the following sections:

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 assign an Internet Protocol version 4 (IPv4) or version 6 (IPv6) to an IP interface or both.

Table 1: Services Enabled by Default on Interfaces

		Enabled by default?	
Service	Default port	Management interface[1]	New interfaces you create
FTP	21	No	No
SSH	22	Yes	No
HTTP	80	Yes	No
HTTPS	443	Yes	No

[1] The “Management Interface” settings shown here are also the default settings for the Data 1 Interface on Cisco C170 appliance .

- If you need to access the appliance via the graphical user interface (GUI), you must enable HTTP and/or HTTPS on an interface.
- If you need to access the appliance for the purposes of uploading or downloading configuration files, you must enable FTP on an interface.
- You can also upload or download files using secure copy (scp).

You can configure HTTP or HTTPS 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 Advanced Network Configuration

Related Topics

- How AsyncOS Selects Default IP Interface, on page 2

How AsyncOS Selects Default IP Interface

AsyncOS selects the default IP interface based on the lowest IP address in which the IP interfaces appear under **Network** > **IP Interfaces** page or in the `ifconfig` CLI command. The first IP interface in the list that resides on the subnet in question is used.

If there are multiple IP addresses configured within the same subnet as the default gateway, the IP address with the lowest number is used. For example, if the following IP addresses are configured within the same subnet,

- `10.10.10.2/24`
- `10.10.10.30/24`
- `10.10.10.100/24`
- `10.10.10.105/24`

AsyncOS chooses `10.10.10.2/24` as the default IP interface.

Configuring FTP Access to the Email Security Appliance

Procedure

Step 1 Use the **Network > IP Interfaces** page or the `interfaceconfig` command to enable FTP access for the interface.

Danger By disabling services via the `interfaceconfig` command, you have the potential to disconnect yourself from the 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 2 Submit and commit your changes.

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

```
$ ftp 192.168.42.42
```

Note Many browsers also allow you to access interfaces via FTP.

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.

Directory Name	Description
/configuration	The directory where data from the following commands is exported to and/or imported (saved) from: • Virtual Gateway mappings (`altsrchost`) • configuration data in XML format (`saveconfig, loadconfig`) • Host Access Table (HAT) (`hostaccess`) • Recipient Access Table (RAT) (`rcptaccess`) • SMTP routes entries (`smtproutes`) • alias tables (`aliasconfig`) • masquerading tables (`masquerade`) • message **filters** (`filters`) • global unsubscribe data (`unsubscribe`) • test messages for the `trace` command • Safelist/Blocklist backup file, saved in the following format: *slbl<timestamp><serial number>.csv*
/antivirus	The directory where the Anti-Virus engine log files are kept. You can inspect the log files this directory to manually check for the last successful download of the virus definition file (`scan.dat`).

Directory Name	Description
/configuration /system_logs /cli_logs /status /reportd_logs reportqueryd_logs /ftpd_logs /mail_logs /asarchive /bounces /error_logs /avarchive /gui_logs /sntpd_logs /RAID.output /euq_logs /scanning /antispam /antivirus /euqgui_logs /ipmitool.output	Created automatically for **logging** via the `logconfig` and `rollovernow` commands. See Logging for a detailed description of each log. See “Log File Type Comparison” for the differences between each log file type.

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 previous table. 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 of `mail3.example.com` .

Note that the command prompts for the passphrase for the user (admin). This example is shown for reference only; your particular 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 appliance .

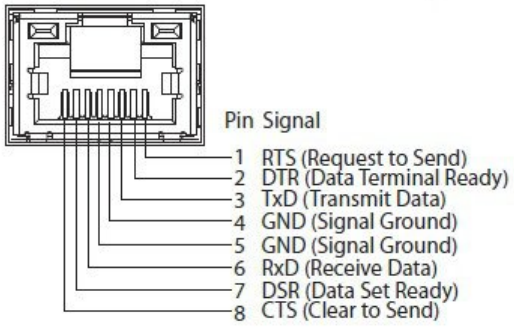
Note Only users in the operators and administrators group can use secure copy (`scp`) to access the appliance . For more information, see Adding Users.

Accessing the Email Security appliance 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.

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 following table defines the pin assignments and interface signals for the serial port connector.

Figure 1: Pin Numbers for the Serial Port

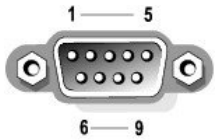


Table 2: Serial Port Pin Assignments

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
9	RI		Ring indicator
Shell	n/a	n/a	Chassis ground