https://www.ciscopress.com/articles/article.asp?p=1687881

CCIE Security v3.0 Quick Reference: Application Protocols

HTTP

HTTP is a request/response protocol between clients (user agents) and servers (origin servers) that is used to access web-related services and pages.

An HTTP client initiates a request by establishing a TCP connection to a particular port on a remote host (port 80 by default). Resources to be accessed by HTTP are identified using uniform resource identifiers (URI or URL) using the http: or https: URI schemes.

HTTP supports authentication between clients and servers, which involves sending a clear-text password (not secure). HTTP is disabled by default on Cisco routers, but it can be enabled for remote monitoring and configuration.

Configuring HTTP

Use the **ip http access-class** command to restrict access to specific IP addresses, and use the **ip http authentication** command to allow only certain users to access the Cisco router via HTTP.

If you choose to use HTTP for management, issue the **ip http access-class** *access-list-number* command to restrict access to specific IP addresses. As with interactive logins, the best choice for HTTP authentication is a TACACS+ or RADIUS server. Avoid using the enable password as an HTTP password.

The **ip http-server** command enables the HTTP server. If a secure HTTP connection is required, **ip http secure-server** needs to be configured on the router. The default HTTP port 80 can be changed by using the command **ip http port** *port-number*. Varying forms of authentication for login can be set using the **ip http authentication** [**enable** | **local** | **tacacs** | **aaa**] command. However, the default login method is to enter the hostname as the username and the enable or secret password as the password. If local authentication is specified by using **username** *username* **privilege** [**0**-**15**] **password** *password*, the access level on the Cisco router is determined by the privilege level assigned to that user.

HTTPS

Secure HTTP or HTTPS provides the ability to connect to a HTTPS server securely. It uses SSL and TLS (transport layer security) to provide authentication and data encryption.

An HTTPS client initiates a request by establishing a TCP connection to a particular port on a remote host (port 443 by default). Resources to be accessed by HTTPS are identified using URIs or URLs using the HTTPS URI schemes.

When a client connects to the secure HTTPS port, he first authenticates to the server by using the server's digital certificate. The client then negotiates the security protocols it will use for the connection with the server and generates session keys for encryption and decryption purposes. If the authentication fails, the client cannot establish a secure encrypted session, and the security protocol negotiation does not proceed.

Configuring HTTPS

Use the **ip http access-class** command to restrict access-specific IP addresses, and use **ip http authentication** to allow only certain users to access the Cisco router via HTTP.

If you choose to use HTTP for management, issue the **ip http access-class** *access-list-number* command to restrict access to appropriate IP addresses. As with interactive logins, the best choice for HTTP authentication is a TACACS+ or RADIUS server. Avoid using the enable password as an HTTP password.

The **ip http secure-server** command enables the HTTPS server. HTTP authentication for login can be set using the **ip http authentication** [**enable** | **local** | **tacacs** | **aaa**] command. All default login methods and local authentication methods supported are the same as mentioned in the section, "HTTP."

The **ip http secure-port** command can set the HTTPS port number from the default value of 443, if required.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is a text-based protocol usually used by two mail servers to exchange e-mail. Users can then retrieve e-mail from the servers via mail clients such as Outlook, Eudora, or Pine. Mail clients use various protocols, such as Post Office Protocol 3 (POP3), to connect to the server.

SMTP uses well-known ports TCP port 25 and UDP port 25. The client and SMTP server send various commands when communicating. Table 3-1 lists some SMTP commands and their purpose.

Table 3-1. SMTP Commands

Command	Function
HELLO (**HELO**)	Identifies the SMTP client to the SMTP server.
MAIL (**MAIL**)	Initiates a mail transaction in which the mail data is delivered to an SMTP server, which is then either delivered to mailboxes or passed to another system via SMTP.
RECIPIENT (**RCPT**)	Identifies an individual recipient of the mail data; multiple use of the command is needed for multiple users.
DATA (**DATA**)	Identifies the lines following the command (such as the **MAIL** command) as the mail data in ASCII character codes.
SEND (**SEND**)	Initiates a mail transaction in which the mail data is delivered to one or more terminals.
SEND OR MAIL (**SOML**)	Initiates a mail transaction in which the mail data is delivered to one or more terminals or mailboxes.
SEND AND MAIL (**SAML**)	Initiates a mail transaction in which the mail data is delivered to one or more terminals and mailboxes.

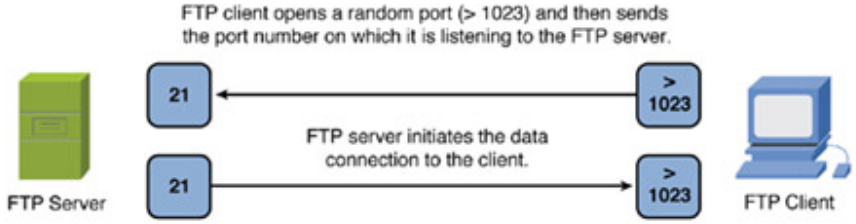
Command	Function
RESET (**RSET**)	Aborts the current mail transaction. Any stored sender, recipients, and mail data must be discarded, and all buffers and state tables must be cleared. The receiver must send an OK reply.
VERIFY (**VRFY**)	Verifies whether a user exists; a fully specified mailbox and name are returned.
NOOP (**NOOP**)	Specifies no action other than that the receiver sent an OK reply.
QUIT (**QUIT**)	Closes the transmission channel; the receiver must send an OK reply.

File Transfer Protocol

FTP allows users to transfer files from one host to another. FTP is a TCP-based connection-oriented protocol, and it uses port 21 to open the connection and port 20 to transfer data. FTP uses clear-text authentication. FTP clients can be configured for two modes of operation: PORT (active) mode and PASV (passive) mode. Figure 3-1 shows FTP modes of operation between an FTP client and FTP server for both the active and passive mode.

Active Mode

In active mode, the FTP client opens a random port (> 1023), sends the FTP server the random port number on which it is listening over the control stream, and waits for a connection from the FTP server. When the FTP server initiates the data connection to the FTP client, it binds the source port to port 20 on the FTP server. Active FTP is less secure than passive mode because the FTP server initiates the data channel, which means opening port 20 to the outside world, which is less secure than using port 21. In active mode, the FTP server initiates the FTP data channel.



Passive Mode

In passive mode, the FTP server opens a random port (> 1023), sends the FTP client the port on which it is listening over the control stream, and waits for a connection from the FTP client. In this case, the FTP client binds the source port of the connection to a random port greater than 1023. In passive FTP, the client initiates both the control connection and the data connection.

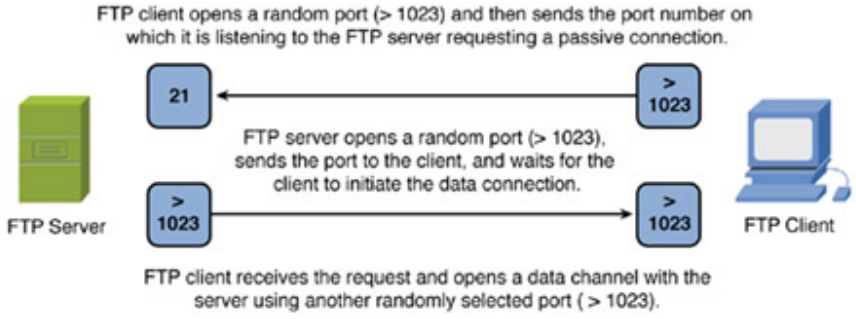


Figure 3-1 Overview of FTP Operation and Operating Modes