



Deep Six Technologies SAS DS200 Installation Guide

Installation Guide

Revision Date : 6 July 2007
Version : 03

Contents

| | |
|---|----|
| DS200 Installation | 3 |
| Requirements | 3 |
| How the DS200 Works | 3 |
| Email Routing Concepts | 4 |
| Preparing for DS200 Configuration | 5 |
| Email Server Settings: | 5 |
| DS200 Settings: | 5 |
| Locating your IP Configuration and Network Settings | 6 |
| DS200 First steps | 7 |
| Phase 1: Connect to the DS200 | 7 |
| Phase 2: Configure the DS200 | 8 |
| Optional Configuration Items | 9 |
| Important Installation Notes | 10 |
| Troubleshooting | 11 |

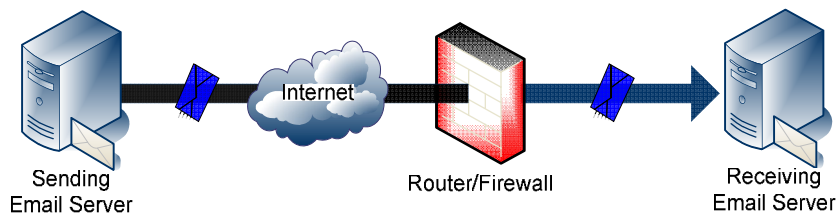
DS200 Installation

Requirements

- DS200
- Power supply (AC adapter) for the DS200 (included)
- An Ethernet cable (not included)
- A 9-pin "null modem" serial cable, female to female (not included)

How the DS200 Works

Normally an email server receives incoming SMTP (email) connections from a sending server. The two servers negotiate and complete the SMTP transaction, which includes transmission and receipt of the email message, as shown below:

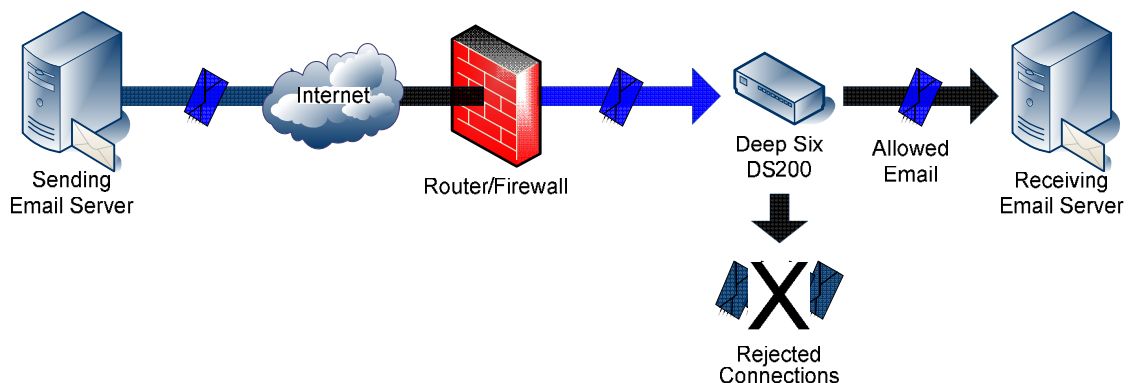


Deep Six's DS200 anti-spam appliance intercepts incoming SMTP connections before they reach the receiving email server. During SMTP connection negotiation, *before an email message is transmitted*, the DS200 decides whether the sending server is a spam source or legitimate.

If the sending server is not a spam source, the DS200 behaves like a router, allowing the sending and receiving servers to negotiate and complete the email transaction.

If the sending server is a spam source, the DS200 acts like a firewall, terminating the SMTP connection before the message is transmitted by the sending server.

The diagram below depicts an email network with a DS200 installed:



Although this diagram shows a typical configuration, the DS200 can be used in many other email network configurations – with or without a firewall, behind a Microsoft Small Business Server, remote or on site, etc. What's important is to understand how email routes to your email server. To assist with less common email configurations, the next section will describe email routing concepts.

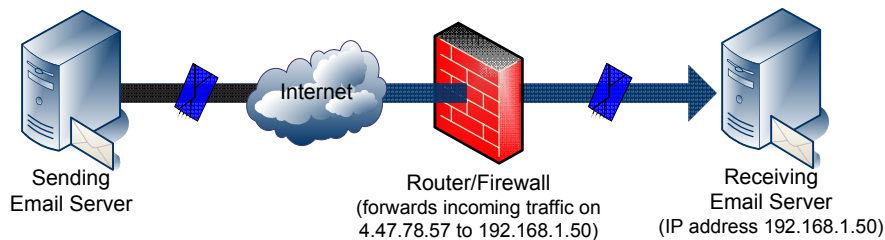
Email Routing Concepts

When trying to send to an email address like person@yourdomain.com, a sending email server uses the Internet's DNS (Domain Name Server) system to look up the IP address of the receiving email server that accepts email for email addresses ending in @yourdomain.com.

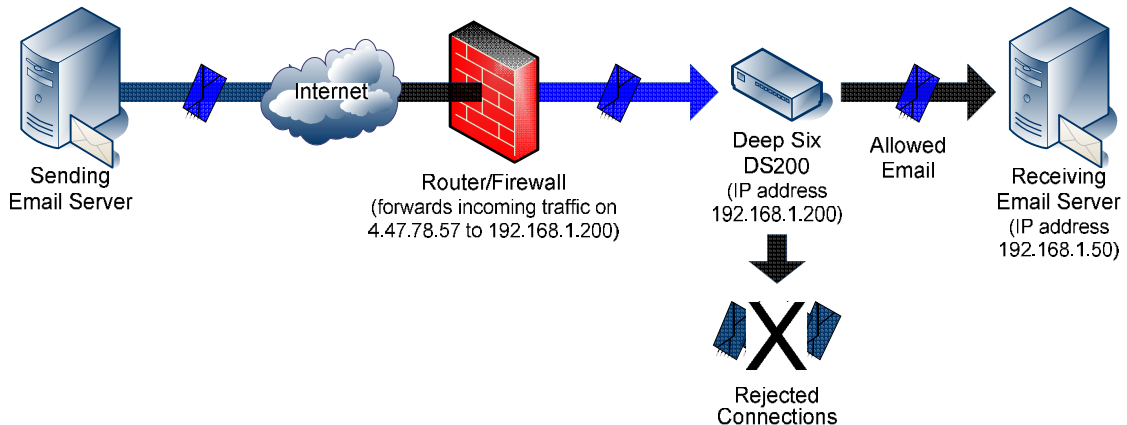
This lookup begins with an "MX record" for the domain, which usually in turn references an "A record" resolving to an IP address. The following is an example of MX and A records:

| Domain | Type | Class | TTL | Answer |
|---------------------|------|-------|-------|--|
| yourdomain.com | MX | IN | 86400 | smtp.yourdomain.com. [Preference = 10] |
| smtp.yourdomain.com | A | IN | 86400 | 4.47.78.57 |

In this case the IP address 4.47.78.57 is the public IP address of the receiving email server. In the diagram below, the router/firewall translates incoming SMTP traffic to the internal network IP address of the email server:



For this example, the simplest way to route email to the DS200 is to change the router/firewall setting to forward incoming SMTP traffic to the DS200, which in turn will route legitimate connections to the receiving email server:



In a configuration without a firewall, the simplest method to route email to the DS200 is to add a new A record resolving to the public IP address of the DS200, and to change the MX record to resolve to that new A record, as follows:

| Domain | Type | Class | TTL | Answer |
|------------------------|------|-------|-------|---|
| yourdomain.com | MX | IN | 86400 | inbound.yourdomain.com. [Preference = 10] |
| smtp.yourdomain.com | A | IN | 86400 | 4.47.78.57 |
| inbound.yourdomain.com | A | IN | 86400 | 4.47.78.200 |

Preparing for DS200 Configuration

The basic configuration for the DS200 involves the following items, explained in more detail in the Installation Instructions section:

1. Connecting to the DS200 via the serial port.
2. Logging in to the default administrator account
3. Configuring the DS200 to work on the network (IP address, netmask, gateway, DNS)
4. Configuring the DS200 to “listen” for incoming SMTP connections and route legitimate connections to the protected email server.
5. Setting the DS200 date and time

Optional but important configuration items include:

6. Configuring the DS200 custom reject message and Webgate.
7. Enabling telnet access for administrator accounts
8. Enabling log access via browser
9. Configuring the DS200 to be more or less aggressive in blocking spam sources

It is recommended to fill in the following worksheet before proceeding to configuration instructions:

Email Server Settings:

A.1) IP Address of your email server: _____

A.2) SMTP Port (Standard inbound mail port is 25): _____

DS200 Settings:

B.1) IP Address:..... _____

B.2) Netmask: _____

B.3) Incoming Email “Listen” Port (standard port is 25): _____

B.4) Gateway IP Address:..... _____

B.5) DNS Server IP Address:..... _____

Once this worksheet is complete and verified, please proceed to the next page for DS200 installation instructions.

Locating your IP Configuration and Network Settings

One way to locate the current network settings, including netmask, gateway IP address, and DNS server IP address, is to use the IPConfig command in the DOS prompt window of a PC on the same network as the DS200.

In Windows you can do this by:

- Click on the Start Menu.
- Select Run.
- Type “cmd” and press <enter>.
- Type “ipconfig /all” and press <enter>.
- This will bring up the data onto the screen in which you can record the data necessary for connecting the DS200 with your network.

DS200 First steps

Phase 1: Connect to the DS200

- 1) Do not connect the power supply until told to do so in this configuration.
- 2) Connect the DS200 to your computer with the null-modem serial cable. If your computer has multiple serial ports, make a note to which COM port you connected (e.g. COM1 or COM2).
- 3) Start Windows HyperTerminal. In WindowsXP, this can be found by clicking: START menu → All Programs → Accessories → Communications → HyperTerminal
- 4) After starting Hyper Terminal, a dialogue box titled "New Connection" will be open. Type "Deep Six" as the name of the connection and select "OK".
- 5) The next box will prompt an area code, phone number and "Connect Using" input. Select "Connect Using" by choosing COM1 or COM2, which corresponds to where you connected the null modem cable. (You do not need to enter phone information)
- 6) You are now prompted with the properties box, select the following:
 - Set "Bits per second" to 19200
 - Set "Data bits" to 8.
 - Set "Parity" to "None"
 - Set "Stop bits" to 1
 - Set "Flow control" to "None"
 - Click the "OK" button.
- 7) After selecting "OK" the properties box closes. In the menu select File → Properties.
- 8) Select the "Settings" tab on the properties window. Under "Emulation" select the drop down list option "VT100". Then select "OK".
- 9) Plug the power supply into a power outlet and connect it to the DS200.
- 10) You should now see in the HyperTerminal window, the DS200 initializing. If you do not, proceed to the "Troubleshooting" section of this guide.
- 11) Connect the Ethernet cable to the DS200 and the network.
- 12) After the DS200 initializes you are prompted to "Enter User ID:" For the first login, enter "Admin" (without quotes) and press "Enter" on your keyboard.
- 13) You are now prompted with "Enter Password:" For the purpose of this initial login, enter the numbers, "01234" (without quotes) and press "Enter" on your keyboard.
- 14) You are now logged in to the DS200 and you may now proceed to initial configuration.

Phase 2: Configure the DS200

Mandatory Configuration Items

Plug the DS200 into the network using the Ethernet cable. Use the Configuration Worksheet information to proceed as follows, where an information item from the worksheet is designated by X.Y.

Configure IP Address:

- 1) Main Menu → **I** → **A**
- 2) Enter IP Address (**B.1**) and press <enter>
- 3) Enter netmask (**B.2**) and press <enter>
- 4) Verify that the information entered is correct and press **Y** <enter>

Configure DNS Server Address:

- 1) Main Menu → **D** → **A**
- 2) Enter DNS server address (**B.5**) above and press <enter>
- 3) Verify that the address entered is correct and press **Y** <enter>

Configure Network Gateway Address:

- 1) Main Menu → **G** → **A**
- 2) Enter Gateway address from (**B.4**) and press <enter>
- 3) Verify that the address entered is correct and press **Y** <enter>

Add Mail Server:

- 1) Main Menu → **M** → **A**
- 2) Enter the short name for this mail server entry and press <enter>
- 3) Enter IP Address (**B.1**) and press <enter>
- 4) Enter port number (**B.3**) and press <enter>
- 5) Enter IP Address (**A.1**) and press <enter>
- 6) Enter port number (**A.2**) and press <enter>
- 7) Enter a name (use no numbers, spaces, or punctuation marks) for the log file folder for this server and press <enter>
- 8) Verify that the information entered is correct and press **Y** <enter>

Configure Time/Date:

- 1) Main Menu → **Y** → **D** → **YYYY:MM:DD HH:MM:SS** (as instructed)

Reboot the DS200:

- 1) Main Menu → **Y** → **B** (You should always reboot when prompted or notified by the banner above the menu)

Update the DS200 firmware to the latest version:

- 1) Type "updatenow" at any menu prompt. If you have correctly configured the DS200 to work on your network, it will download the latest firmware and reboot. This process should take less than 2 minutes before you are able to log in again.

Management Users:

- 1) Main Menu → **U** → **A**
- 2) Enter management user ID and press <enter>
- 3) Enter management user password and press <enter>
- 4) ***Record the user ID and password in a secure location***
- 5) When ready delete the pre-configured admin account, to secure your box. Do this by selecting option 3 (Delete Management User) under Management User Configuration. **Make sure that you have created an additional account prior to deleting the preconfigured admin account and have the user and password info recorded!**

Router/Firewall Configuration

If the DS200 has been installed behind a router or firewall, it will be necessary to configure the router/firewall to forward/translate incoming SMTP connections to the DS200. For example, in the Email Routing Concepts section of this Installation Guide, a diagram shows a firewall translating port 25 traffic on the external IP address 4.47.78.57 to 192.168.1.200. Once your router/firewall has been configured to forward/translate SMTP traffic to the DS200, and the DS200 has been completely configured, the DS200 will begin protecting your email server from spam.

Note: In cases where the IP address of the DS200 was previously assigned to another device, it may be necessary to refresh the router table cache (also known as ARP cache) in the router or firewall. Otherwise traffic will not route to the DS200, and no email will reach your email server. Usually this is done by logging in to the administrative console of the router/firewall, but in some cases a router/firewall restart is required.

Optional Configuration Items

Management Port: (For Remote Access)

Activate the management port if you want to remotely access the DS200.

- 1) Main Menu → **P** → **A**
- 2) Enter management IP Address (**B.1**) <enter>
- 3) Enter management port <enter> (e.g. 8484)
- 4) If you add a management port make sure you have created a new secure user account and deleted the preconfigured account, which is standard among all DS200 boxes.
- 5) Access the DS200 by entering "telnet IPADDRESS PORT", where IPADDRESS is the management IP address, and PORT is the management port. When you connect, you will be prompted for username and password.

Configure E-Mail Webgate and Custom Reject Message

- 1) Please see the Webgate Configuration Guide, provided as a separate document.

Maximum Accept/Reject Score:

- 1) Main Menu → **Y** → **A**
- 2) The initial default is set at 20, a moderate setting. Lower numbers are more aggressive but may result in temporary false positives that require whitelisting of blocked, legitimate IP addresses. If the Webgate feature is configured and verified, a setting of 15 is generally recommended after verification of successful DS200 operation.

HTTP Log Access:

Setting up HTTP log access allows browser-based access to DS200 transaction logs.

- 1) Main Menu → **H** → **A**
- 2) Enter the IP address that you want to use for browser access to the logs. This can be the same IP address from B.1 of the Configuration Worksheet.

Enter the port that you want the DS200 to use to accept log viewing requests (e.g. 8686).

- 3) After completion, you will be returned to the HTTP Log Server Configuration Menu. Use → **M** → **Y** → **B** to return to the main menu, enter the System Configuration Menu, and reboot the DS200.
- 4) After reboot, to access the logs, enter the following URL in your browser (where IPADDRESS is the IP address from step 2 above, and PORT is the port number from step 3):
http://IPADDRESS:PORT/mlogs

Important Installation Notes

SMTP Mail Server Security Practices

Open relay protection should be maintained on the server. As consistent with industry-accepted security practices, your mail server should require user-based authentication (SMTP AUTH) for mail relay (for accepting mail for delivery outside the network), *not* IP address-based authentication.

Multiple MX Records

If you have multiple MX records for redundancy, either configure all MX records to resolve to the DS200, or delete all MX records except one that resolves to the DS200. If there remain MX records that resolve elsewhere, spammers will use these alternate MX records to route junk email to your email server – regardless of the priority levels of the alternate MX records. Keep in mind that modern SMTP servers will typically retry for up to 24 hours if your primary email server is down. Therefore it's not typically required to use an MX record to route to a backup email server at your ISP, unless you expect outages of the primary server for more than 24 hours at a time.

Firewall SMTP Issues

Certain firewalls, including some models from Cisco, Watchguard, Checkpoint, and Raptor, have SMTP Proxy capabilities or "SMTP fixup" features that may not permit email to flow correctly between certain email servers (including Microsoft Exchange). To resolve, turn off any firewall features (e.g. Cisco PIX's "MailGuard" feature) that prevent transmission of ESMTP commands such as EHLO, etc. Microsoft Knowledge Base article 320027 contains more information about this issue.

Troubleshooting

Problems Connecting with HyperTerminal

If you plug in the power to the system after step 10 of Phase 1, and you do not see data in the HyperTerminal window, use these strategies.

1. Press Enter on the keyboard of the computer connected to the DS200 by null modem serial cable. If this does not result in a prompt to "Enter User ID:" then proceed to the next step.
2. Make sure the cable connected between the DS200 and your computer is a null modem cable. If it is a serial cable you must have a null modem adapter.
3. If you still do not see any information go back to step 8 and check that the terminal emulation is set to "VT100". If it is, click the "Cancel" button on the "Properties" dialog box and try the following:
 - a. On the Hyper Terminal "Call" menu, select "Disconnect". The session will disconnect.
 - b. On the Hyper Terminal "File" menu, select "Properties". On the "Connect To" tab will be a button labeled "Configure", below the "Connect using" field. Click this button.
 - c. Verify that the COM port is configured as described in Step 10. If it is not, set the fields correctly and click the "OK" button. On the Hyper Terminal "Call" menu, select "Connect". Press the "Enter" key on your keyboard. If you see a response such as "Enter User ID:", proceed to step 15. If you do not see any response, you may have the null modem cable plugged into a different serial port than you have entered. In this case, use the "Call" menu to disconnect the session again. On the Hyper Terminal "File" menu, select "Properties". On the "Connect To" tab, select a different serial ("COM") port and click the "OK" button. Then use the "Call" menu to connect again, and press the "Enter" key on your keyboard. You should now see a response from the DS200. If you do not, try each serial port until you see a response.

Email Traffic Not Reaching the DS200

In cases where the IP address of the DS200 was previously assigned to another device, it may be necessary to refresh the router table cache (also known as ARP cache) in the router or firewall. Otherwise traffic will not route to the DS200, and no email will reach your email server. Usually this is done by logging in to the administrative console of the router/firewall, but in some cases a router/firewall restart is required.

Firewall SMTP Issues

Certain firewalls, including some models from Cisco, Watchguard, Checkpoint, and Raptor, have SMTP Proxy capabilities or "SMTP fixup" features that may not permit email to flow correctly between certain email servers (including Microsoft Exchange). To resolve, turn off any firewall features (e.g. Cisco PIX's "MailGuard" feature) that prevent transmission of ESMTP commands such as EHLO, etc. Microsoft Knowledge Base article 320027 also contains information about this issue.

Other Problems

For other problems, or help installing your DS200, please contact support@d6tech.com.