


# Monitoring All Windows Traffic with Burp Suite

 [fr0stb1rd.gitlab.io/posts/Monitoring-All-Windows-Traffic-with-Burp-Suite](https://fr0stb1rd.gitlab.io/posts/Monitoring-All-Windows-Traffic-with-Burp-Suite)

December 27, 2024



Burp Suite is a powerful tool used for testing the security of web applications. One of its main features is the ability to capture and analyze network traffic. In this article, we will show you how to set up Burp Suite to monitor all traffic on a Windows computer.

## What is Burp Suite?

Burp Suite is a platform that provides tools for testing the security of web applications. It allows users to capture HTTP/S requests, analyze responses, and change data in transit. This makes it an important tool for security professionals and developers.

# Setting Up Burp Suite for Windows Traffic Monitoring

---

To monitor all Windows traffic with Burp Suite, follow these steps:

## Step 1: Install Burp Suite

---

1. Download the latest version of Burp Suite from the official website.
2. Install the application by following the instructions on the screen.

## Step 2: Install Burp's CA Certificate

---

To capture HTTPS traffic, you need to install Burp's CA certificate before setting up the proxy.

1. In Burp Suite, go to the "Proxy" tab and click on "Intercept" to make sure it is off.
2. Go to "Proxy" > "Options" > "Import / export CA certificate".
3. Export the certificate in DER format.
4. Open Windows Certificate Manager (run `certmgr.msc`).
5. Import the certificate into the "Trusted Root Certification Authorities" store.

## Burp Suite CA Certificate Installation Steps

---

1. **Launch Burp Suite:** Open the Burp Suite application.
2. **Download the Certificate:**
  - Open your browser and go to the Burp Suite proxy listener port, which is usually `http://127.0.0.1:8080`.
  - Click on "CA Certificate" in the top-right corner to download the certificate named "cacert.der".
  - You may see a warning that the file type is unsafe; accept the warning.
3. **Install the Certificate:**
  - Double-click on the downloaded "cacert.der" file and accept the security warning.
  - In the certificate viewer window, click "Install Certificate".
4. **Choose Installation Options:**
  - **Important:** To monitor all network traffic, select "Local Machine". This makes the certificate trusted for all users.
  - If you choose "Current User", it will only be valid for that user, and you cannot monitor traffic for other users.
  - Manually set the certificate to be placed in the "Trusted Root Certification Authorities" store.
  - Click "Finish" to complete the import.
5. **Restart Browsers:** To make the changes work, restart your browsers. This should affect all browsers on your computer, but you may need to add the certificate to specific browsers like Firefox if they use their own trust store.

**Note:** If you want to capture network traffic from another device, it will need to import your specific Burp certificate, as each installation creates a new certificate.

## Step 3: Configure Proxy Settings

---

Burp Suite works as a proxy server, so you need to set up your Windows system to send traffic through it.

1. Open Burp Suite and go to the “Proxy” tab.
2. Click on “Options” and note the proxy listener settings (default is 127.0.0.1:8080).
3. Go to Windows Settings > Network & Internet > Proxy.
4. Turn on “Manual proxy setup” and enter the Burp Suite proxy address (127.0.0.1) and port (8080).

## Additional Configuration via Internet Options

---

From Control Panel/Windows Start Menu, search for “Internet Options” and follow these steps:

1. Internet Options > Connection > LAN settings.
2. Uncheck “Automatically detect settings” and “Use automatic configuration script”.
3. Check “Use a proxy server for your LAN” and provide the address as “127.0.0.1” and port as “8080” (or whatever address and port you have set in Burp proxy options).
4. Make sure the option “Bypass proxy server for local addresses” is unchecked to capture all communication.
5. Click the OK button for all open windows.

Note: You will be able to capture all communication except for some applications that have a built-in proxy or VPN.

## Step 4: Configure Browser Settings

---

To make sure your browser sends traffic through Burp Suite:

1. Open your web browser and go to the proxy settings.
2. Set the proxy to use the same address and port as configured in Burp Suite (127.0.0.1:8080).
3. Make sure that the browser is set to use the system proxy settings.

## Monitoring Traffic

---

Once you have completed the setup, you can start monitoring traffic:

1. In Burp Suite, go to the “Proxy” tab and click on “Intercept” to turn it on.
2. Open your web browser and start browsing. Burp Suite will capture all HTTP/S requests and responses.
3. Analyze the traffic in the “HTTP history” section of the Proxy tab.

## Conclusion

---

By following these steps, you can effectively set up Burp Suite to monitor all traffic on your Windows machine. This setup is very useful for security testing and understanding how web applications communicate over the network. Always remember to use these tools responsibly and within legal limits.

*This article is for educational purposes only and aims to provide a technical understanding of using Burp Suite for network traffic monitoring.*