CHAPTER 9

Guest Activity Logging

Guest Activity Logging provides the ability for the Cisco NAC Guest Server to receive syslog information from network devices such as Firewalls, Proxy Servers and Routers. This information can provide details on all the connections that a guest has made and Layer 7 information such as URLs accessed, depending on the network device.

Guest Activity Logging relies on knowing the IP address for each guest as they authenticate to the network. The Cisco NAC Guest Server receives this information from RADIUS accounting, so you need to configure the network device that the user authenticates through to send this information. Commonly, this is the Wireless LAN Controller or Cisco NAC Appliance. Refer to the information in Chapter 8, "Configuring RADIUS Clients" for details on adding these devices as a RADIUS client.

Note Guest Activity Logging relies on correlating the syslog information with the IP Address received from RADIUS accounting. This means that it will not work if you use a deployment method where the guest's IP address changes after authentication and no additional RADIUS accounting messages are sent.

Once the Cisco NAC Guest Server has the IP Address of each of the guests, then it needs to receive syslog information from the network devices. You should configure each of your network devices to send syslog to UDP port 514 on the Guest Server. The Guest Server then processes the syslog information and correlates it against each guest. This correlation enables you to view the guest's activity on the guest activity log details page for each guest as described in Reporting on Guest Users, page 17-19.

Guest Activity is correlated into individual files that are stored on the disk of the appliance. The appliance can store log files until less than 30% disk space remains; it then either deletes the oldest log files or archives the log files to an external FTP server as described in Configuring Syslog Monitoring Settings, page 9-1.

Note For the report to show the list of URLs visited by guest users, you need to enable HTTP traffic inspection on the NAD. This is not applicable for WLCs.

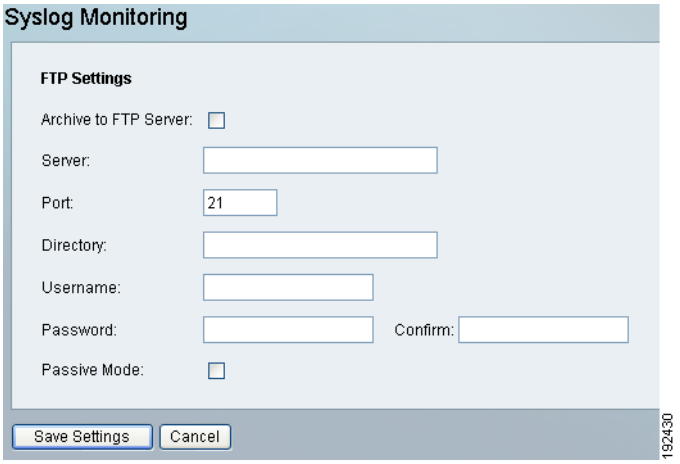
Configuring Syslog Monitoring Settings

Archiving of logs to an FTP server provides the ability to store logs for long periods of time, and also provides the ability to back them up.

When viewing the logs through the sponsor interface, the NAC Guest Server automatically searches for logs on the archive server and displays them in the report for you.

Step 1 From the administration interface, select **Devices > Syslog Monitoring** from the left hand menu as shown in Figure 9-1.

Figure 9-1 Syslog Monitoring



Step 2 If you want to configure the NAC Guest Server to archive guest logs, check the **Archive to FTP Server** checkbox.

Step 3 In the Server field, enter the name or IP address of the FTP server.

Step 4 Enter the Port of the FTP server

Step 5 Specify the Directory on the FTP server where you want the archive files to be stored.

Step 6 Enter the Username and Password for an account that has the ability to log in to the FTP server and has write permissions to the directory specified.

Step 7 By default, the FTP mode used is Active FTP. If you want to use Passive mode, check the **Passive Mode** checkbox.

Guest Activity Logging with Replication Enabled

If you have a pair of NAC Guest Servers replicating database information for resilience, then the guest activity logs are not replicated between each box.

However, if you view the report in the Sponsor interface, the NAC Guest Server contacts the replication box and retrieves the logs from there. It then displays all logs in a consolidated view.

This enables you to have some network devices send syslog to one NAC Guest Server and some to another, but then view all the results through a single interface.

Each NAC Guest Server retrieves the logs from the other Guest Server in the replication pair securely over HTTPS. Each NAC Guest Server must trust the certificate of the other NAC Guest Server so that the retrieval can occur properly. To enable this, ensure that the root CA certificate for the other NAC Guest Server is uploaded as described in Uploading Certificate Files, page 3-14.