

AREN Network Monitoring and Auditing

ASA can provide clients with the local monitoring of all LAN and/or WAN network activity in a school or an entire school system. Monitoring network traffic has many benefits such as providing much needed data that can be used in troubleshooting and in better managing of a network's resources and traffic flow. When a network is experiencing slowdowns this data can provide insight into what might be causing the problem such as a virus-infected desktop or a hacked server.

The traffic monitoring and logging is done by a monitoring server, which uses a side-scanning approach for collecting its data. Side-scanning occurs when the server is placed somewhere within the network where it can view all the data needed to be monitored, but does not slow the traffic or alter it in any way and can be taken off the network without interfering with the network traffic at all. This approach is faster, more efficient, and safer than the inline approach where all traffic must flow through the server, which may lead to a traffic bottleneck. Another disadvantage to an inline server is that it becomes a single point of failure in the network and will cause all network traffic to cease if the monitoring server is not working correctly.

Monitoring Network Traffic with Open-Source Applications: IPAudit and IPAudit-Web

The monitoring server is built using an open-source application called IPAudit. The IPAudit application listens for activity on a network interface placed in promiscuous mode. This interface is usually a high-speed port on a switch that has the ability to span multiple ports over one interface. Once spanned, the interface then has a copy of every packet that is sent through the entire switch. IPAudit is able to watch every unique connection that travels through this interface, but can also be configured to log only certain subnets and not every connection.

The web-based reporting capabilities are added through the coupling of IPAudit and another open-source project called IPAudit-Web. IPAudit-Web allows detailed reporting and viewing of all logged network activity through a user-friendly, web-based interface. The main page of the IPAudit-Web site is shown in **<Figure 1>**. This site can be set up for local or remote viewing with transport-encrypted data through SSL (Secure Socket Layer).



Figure 1

Reports and Graphs Provided by IPAudit-Web

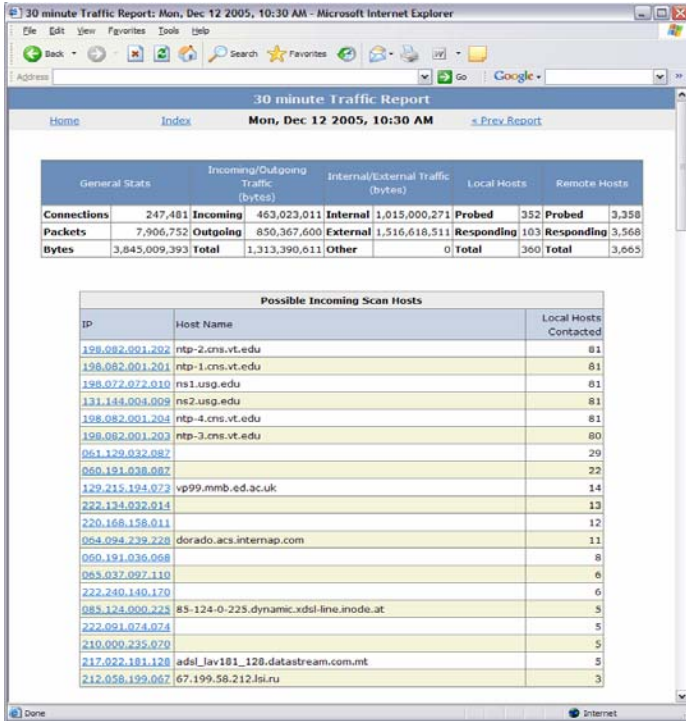


Figure 2

IPAudit-Web provides graphs, tabular data, and html reports for some commonly logged session types. Such session types include incoming/outgoing traffic, internal/external traffic, local-host count (possible incoming scans), remote host count (possible outgoing scans), busiest local machines, and busiest remote machines. An HTML table displaying a list of possible incoming scans along with the number of internal hosts scanned is shown in **<Figure 2>**. A list of possible outgoing scans may also be viewed, which might cause virus-infected machines to stand out from normal machines.

An example of what an atypical graph for internal and external traffic may look like is shown in **<Figure 3>**. An atypical graph for current incoming and outgoing network traffic is shown in **<Figure 4>**. You can notice the weekends are the valleys and the weekdays are the peaks.

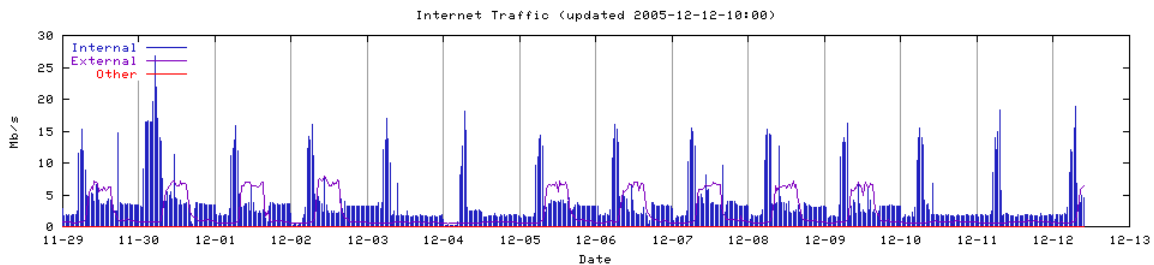


Figure 3

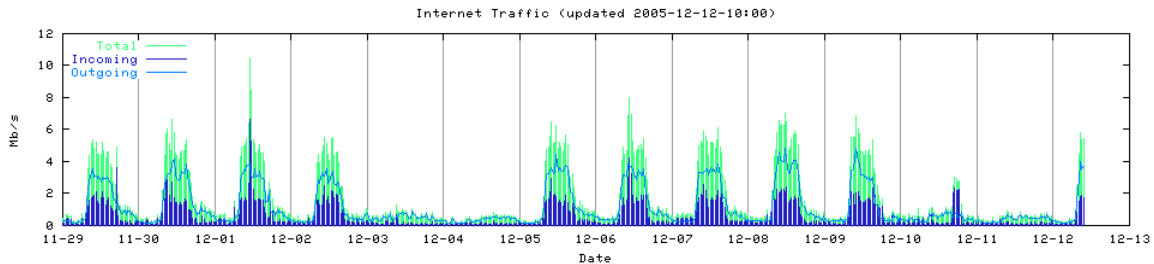


Figure 4

IPAudit-Web Provides Network Traffic Analysis Tools

IPAudit-Web provides the ability to search for unique session instances by such things as IP address, used ports, time frames, protocols, and the first and last talker. A search for a single node of 129.66.20.7 is shown in **<Figure 5>**. When a specific node is identified to be causing trouble, such as using an abnormal amount of network traffic for a particular time period, this report can be very useful. One can view the identified node's traffic patterns broken down into time periods, which could help identify the first occurrence of the traffic anomaly. The starting time-period may help to pinpoint the identified node's problem, such as a hacked server sharing movies and games over the Internet.

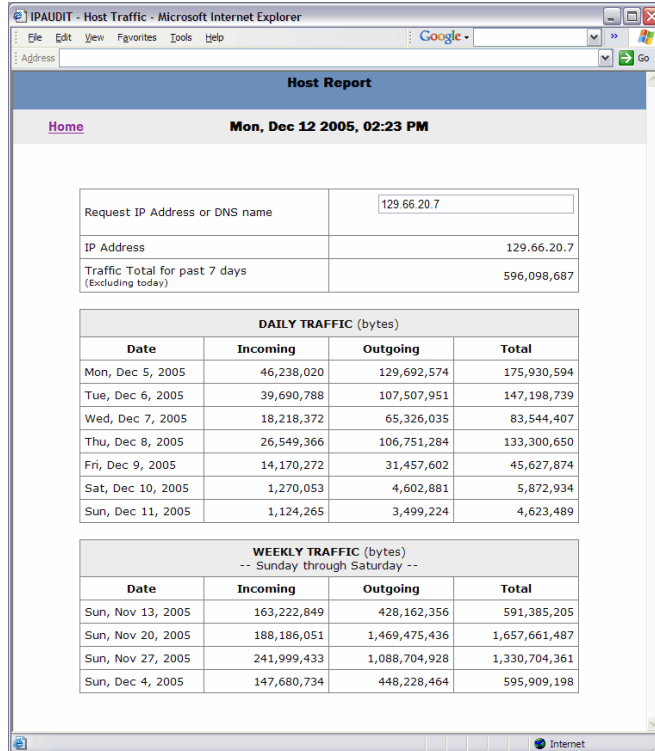


Figure 5

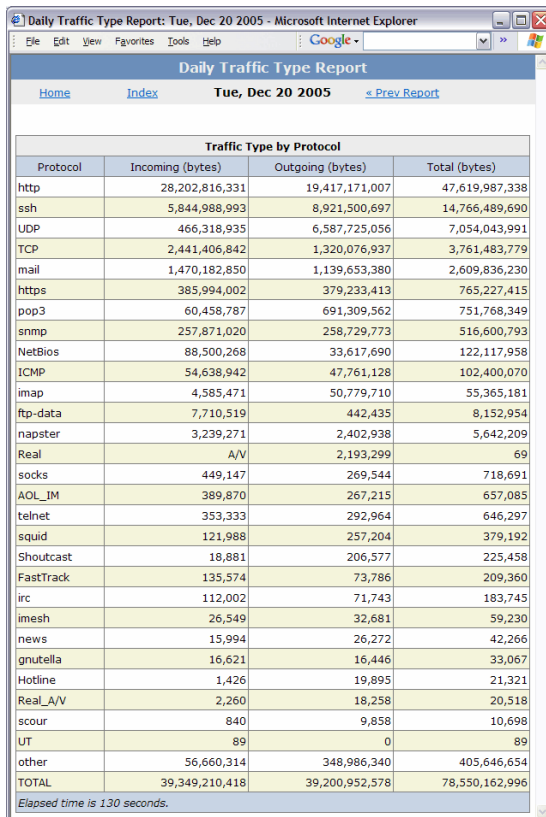


Figure 6

IPAudit-Web provides a daily breakdown of network traffic by protocol, incoming bytes, outgoing bytes, and total bytes **<Figure 6>**. This view is very helpful in identifying the underutilizations and abuses of a network's resources. This information will also provide for better troubleshooting when trying to identify certain traffic-shaping problems or in the consideration of firewall ACLs (Access Control Lists). This table (Figure 6) shows that the most used protocol on this WAN is web traffic (http). It also shows that there is some P2P (Peer to Peer) traffic traveling the network such as the following: Shoutcast, gnutella, napster, FastTrack (Kazaa, Grokster, etc.), Hotline, and imesh protocols. The amount of P2P traffic may be acceptable for some networks and not for others. Acceptability depends on the amount of the network's total bandwidth, the protocols used, and the ability of the network to control this traffic.

ASA Offers Several Different IPAudit/IPAudit-Web Configurations

ASA offers several different IPAudit/IPAudit-Web configurations, which are dependent upon the network(s) used to monitor activity and the equipment on which it is configured. Some possibilities include the purchase of a new server with an IPAudit system in place, or the purchased service of a Systems Analyst to install and configure IPAudit on one of the clients existing machines. Other services are available at the client's request.

We have created and/or installed IPAudit servers at the following locations:

1. Alabama A&M University
2. Baldwin County Schools
3. Chilton County Schools
4. Dauphin Island Sea Labs
5. Scottsboro Schools

References:

<http://ipaudit.sourceforge.net/ipaudit-web/>

***** IPAudit is a free network-monitoring program available and extensible under the GNU GPL. For more, see License Information. *****