View Intrusion Prevention System (IPS) Report on a WRVS4400N Wireless-N Gigabit Security Router

Objective

The Intrusion Prevention System (IPS) protects your network services, such as Web and Instant Messages, and also defends you against possible vulnerabilities, such as viruses, worms, and possible backdoor exploits. IPS monitors the network traffic for malicious or unwanted behavior, and if an attack is detected, it drops those malicious packets to protect the network while the rest of the traffic passes through the network. IPS allows you to stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped in real time.

This article shows the report that the WRVS4400N generates for the current vulnerabilities of the system, this gives you the necessary information to take control of that issue in the network.

Applicable Devices

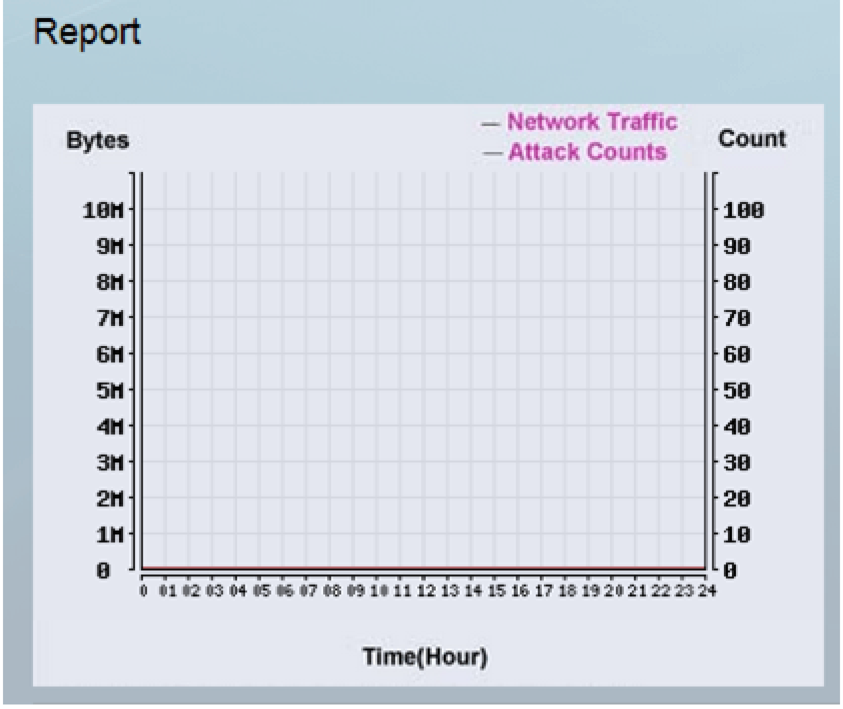
- WRVS4400N

Software Version

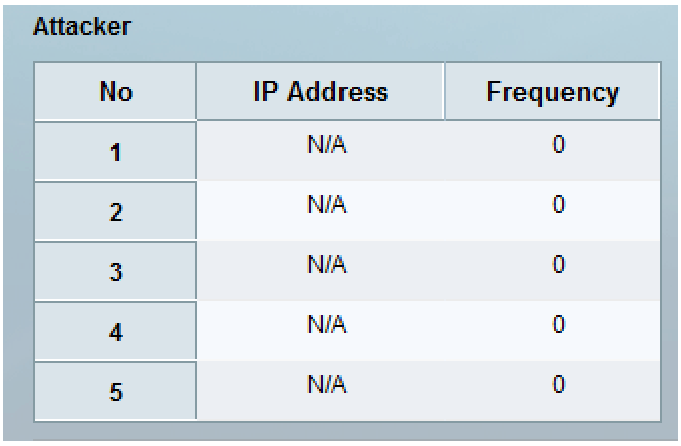
- v2.0.1.3

Intrusion Prevention System Report

Step 1. Log in to the web configuration utility and choose **IPS > Report**. The *Report* page opens. The report page displays three sections Report, Attacker, and Attacked Category.



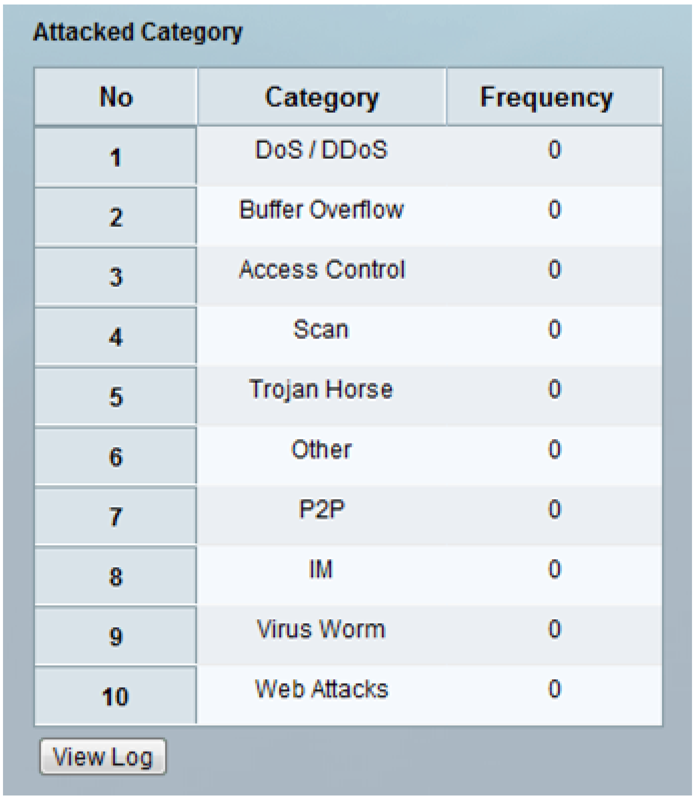
- Report Diagram — A graph that displays the network traffic and the number of attacks in the last twenty-four hours.



Attacker

No	IP Address	Frequency
1	N/A	0
2	N/A	0
3	N/A	0
4	N/A	0
5	N/A	0

- Attacker — Displays the IP addresses of attackers and the number of times they occurred in a table.



Attacked Category

No	Category	Frequency
1	DoS / DDoS	0
2	Buffer Overflow	0
3	Access Control	0
4	Scan	0
5	Trojan Horse	0
6	Other	0
7	P2P	0
8	IM	0
9	Virus Worm	0
10	Web Attacks	0

- Attacked Category — Displays the type of attack and the number of times it occurred in a table.

  – DoS / DDoS — Denial of Service (DoS) prevention increases network security. DoS and DDoS attacks flood the network with additional requests that limit the availability of network resources.

  – Buffer Overflow — A buffer overflow attack takes palace when a certain quantity of data from a program or process is stored in the temporary memory, this data contains malicious codes that attacks the network and the computer.

  – Access Control — Access control attack takes place when the application of the access control fails and the access data can be broken to enter to a network or device.

  – Scan — Port scan attack takes place when a malicious code is sent to a port in a device to test its status. This information is used by the attacker to understand the weaknesses of the device.

  – Trojan Horse — A Trojan horse, or Trojan, is a malicious code that is is hidden in a legitimate program or file. When this file or program is accepted by the user, the malicious code attacks the device or the network.

  – Other — Other kind of attacks that the network or the device can suffer.

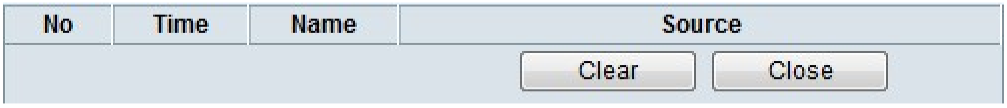
  – P2P — A peer-to-peer (P2P) network is similar to a client-server network where each computer acts as a server and a client. The P2P attack prevents the communication between the computers in the network which leads to loss of information and conflicts in the network.

  – IM — Instant-messaging attacks take place when the user receives a malicious code in an instant message in a chat session. This malicious code attacks the device and the network.

– Virus Worm — A computer worm is a malicious code that has the capacity to replicate itself in a network. This infects each computer and uses the network as a mechanism to propagate.

– Web Attack — Is when a website has a malicious file that attacks the network or the device .

Step 2. Click the **View Log** button to view the log. These are the messages that the system generates when the network is under attack.



No	Time	Name	Source

- Number No — Displays the number of times that the attack occurred in the system.

- Time — Displays the time when the attack occurred

- Name — Displays the name of the attack

- Source — Displays the source of the attack

Step 3. Click the **Clear** button to clear the log table.