Is SenderBase on the Cisco Email Security Appliance (ESA) another DNS RBL?

Contents

Question
Answer
Related Information

Question

Is SenderBase on the Cisco Email Security Appliance (ESA) another DNS Real-time Blackhole List (RBL)?

Answer

SenderBase is no ordinary DNS RBL. In the anti-spam community, there are many DNS-based blocklists. A technique developed over the years, DNS-based blocklists provide a way of adding a standardized API (application programming interface) to a widely distributed database. Because network devices, such as mail servers, all have a DNS client application built-in (sometimes called a 'resolver'), using the DNS to look up information about IP addresses is a very natural operation for most systems. The idea of a DNS-based blocklist is to provide an easy way for a widely distributed community of users to efficiently query an IP-oriented list without having to worry about database replication, authentication, or more elaborate APIs.

Most DNS-based blocklists' strategy is to state some description of a blocklist (e.g., "systems which are known to be open relays") and then allow anyone to query the list to see if an IP address is on the list. If the address appears, then the list owner asserts that the IP address has met the qualifications to be on the list. In other words, DNS-based blocklists are "yes/no" answers---you either are on the list, or you are not.

Volunteers generally manage DNS-based blocklists (although there are few available on a for-pay subscription basis). They also tend to be very idiosyncratic in their operation. As volunteer-run projects, they are operated by individuals or groups who feel very strongly about spam's problem and generally tend to err on the side of blocking legitimate mail. Enterprises who have chosen to use DNS-based blocklists either find them minimally effective for reducing spam (i.e., it's hard to get on the list and the list updates are not timely) or they find that these lists generate a very high false-positive rate (i.e., it's too easy to get on the list).

SenderBase was created to reduce idiosyncratic behavior in DNS-based blocklists and allow the network manager to make their own decisions about how conservative or how aggressively they will use the list. With proper use of SenderBase, in conjunction with an ESA's throttling capabilities, the rate of false positives can be dropped dramatically. At the same time, a large proportion of spam is kept out of the corporate network.

Related Information

- **How does SenderBase work?**
- **Technical Support & Documentation - Cisco Systems**