

SOLUTION NOTE

DNS Architecture

In general, an organization's DNS architecture should be designed (and documented!) to provide maximum resiliency and performance without sacrificing security. Here is a list of important architectural recommendations:

Internal and external name servers should be separated. Internal name servers (those that serve internal clients on PCs and other equipment) should be separated from external (e.g., Internet facing) name servers such as authoritative name servers and forwarders. Allowing internal name servers to communicate directly with Internet name servers could allow a hacker who can exploit a vulnerability in a name server implementation to gain access to the Internet network.

External authoritative name service and forwarding should be separated onto different physical name servers. Separating the two varieties of external name servers allows both to be secured more effectively, and separates these two critical functions.

Stub resolvers shouldn't be allowed to query Internet name servers directly. Stub resolvers, such as those included in Windows and MacOS operating systems, should be forced to query internal name servers. These operating systems can become infected by Trojan horses and other malware that reconfigures their stub resolvers to use Internet name servers. These name servers, in turn, direct these OSes to proxy servers, which can capture users' network traffic, including logins, passwords, credit card numbers, etc.

Border routers or Internet firewalls should employ ingress filtering. An organization's border routers or Internet firewalls should be configured to drop and log all network traffic they receive on external network interfaces that claims to originate from the organization's own address space. This allows administrators to extend trust to addresses in their own address space safely.

Organizations with more than a trivial (ten or fewer) name servers should use forwarders for any Internet name resolution. Forwarders, which serve as Internet proxy servers, allow organizations to compartmentalize their risk to a small set of name servers that communicate directly with Internet name servers, and to focus their attention there. If forwarders are used, internal name servers (i.e., non-forwarders) should not be allowed to query Internet name servers directly.

Organizations should employ architectures that eliminate single points of failure. For example, organizations should avoid placing all authoritative name servers or forwarders on the same subnet, or behind the same router or firewall. Organizations that use forwarding should deploy redundant forwarders.

Critical name servers should be deployed in highly available configurations. Name servers whose operations are critical, such as forwarders and important primary name servers, should be deployed in configurations that guarantee their availability, such as high availability pairs or anycast groups.

Network traffic to and from Internet-accessible name servers should be filtered by a border router or firewall. The filter should allow only legitimate DNS traffic between the name servers and the Internet.

DNS Infrastructure

DNS infrastructure chiefly comprises the name servers that resolve domain names on behalf of an organization's internal clients and name servers that advertise the organization's domain names to clients on the Internet. Here is a list of infrastructure recommendations:

SOLUTION NOTE

Name servers should run on hardware dedicated to that service. That is, a name server should generally not be run on a multiuser system, file server, Domain Controller, or any host not dedicated to supporting core network services. Running a name server on a host that's not dedicated to the task opens the possibility of resource starvation (e.g., running out of disk space on a file server), compromise from user privilege escalation, and much more.

Organizations should secure the operating systems supporting name servers. This includes upgrading the operating systems to the latest, supported versions, patching or applying Service Packs in a timely manner, disabling unnecessary services, implementing host-level packet filtering, and running the name server with least privilege.

Name servers should run the latest name server software, or at least software with no known vulnerabilities.

Name Server Configuration

Name servers whose sole function is to provide authoritative name service, particularly external authoritative name servers, should have recursion disabled.

Forwarders should use access controls to limit recursion to internal clients.

Dynamic updates should only be used when necessary. Any authoritative name server that hosts zones that don't require dynamic updates should deny all updates. When dynamic updates are necessary, they should be secured using TSIG keys. Dynamic updates should not be authorized by source IP address.

Name servers should be configured not to reveal their version. BIND name servers, by default, will reveal their version in response to certain queries. BIND name servers should be configured not to respond with their version, as this allows hackers to quickly identify name servers running a particular version of code, which may be vulnerable.

Name Server/DNS Management and Operations

Hostmasters (those responsible for an organization's DNS and name server management) should subscribe to mailing lists or follow newsgroups as necessary to track the release of new versions of name server software and the discovery of vulnerabilities.

Organizations, particularly those who use BIND, which is open source software, should ensure that they have commercial support for that software. Organizations should ensure that they have sufficient internal expertise to manage and support DNS. Organizations should also ensure that they have sufficient redundancy in the administration of DNS.

The ability to configure and manage name servers and change zone data should only be extended to authorized administrators. If possible, organizations should use fine-grained authorization mechanisms to restrict even those administrators to aspects of configuration they're authorized to modify.

All DNS configuration changes should be logged and archived, along with the initiator and time of the change.

Name servers' log output should be monitored; significant logged events should trigger alerts.

Organizations should have disaster recovery plans that meet recovery time objectives for DNS as a service and for critical name servers.

Organizations should document their DNS architecture, including the locations, addresses and configurations of all name servers.