

DNS Threat Mitigation in Service Provider Environment

A Technical Case Study by Nixu Software

December 2011

Copyright © 2011 Nixu Software

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners.

DNS Threat Mitigation in Service Provider Environment

by Nixu Software, December 2011

Any comments relating to the material contained in this document may be submitted to:

Nixu Software
keilaranta 15, P.O.Box FI-02151
Espoo, Finland.

or by email to:

info@nixusoftware.com

Technical Case Study

Conemedia needed to take some serious action against the alarming number of DoS attacks on its DNS servers.

Business Challenges:

1. Monitor and analyse

DNS servers

2. Mitigate threats

3. Automate DNS management and provisioning

4. Centrally manage remote integrated servers

1. Customer Profile

Conemedia (company name has been changed in order to protect customer privacy) is one of the largest national cable, Internet and telephone operators in Latin America. In the third quarter of 2011, Conemedia had close to 2 million unique subscribers. Its product portfolio includes cable TV, high-speed Internet and digital telephony subscriptions along with a myriad of other services for enterprises and telecommunications companies. With a quality policy aimed at exceeding the clients' expectations, Conemedia is a front-runner in investing in and utilizing cutting edge technology to improve the quality of its service and offerings.

2. Business Challenges

Social media, peer-to-peer networks and IP-everywhere are having a significant impact on DNS platforms run by mobile and fixed Internet Service Providers (ISP). Given the increasingly interactive use of the Internet, the number of DNS queries served out by ISPs have multiplied over the recent years. This trend is expected to continue over the coming years, calling for careful re-evaluation of DNS platform strategies required to scale up the operations without eroding the service level.

DNS security is another issue that has become of critical importance to ISPs. The increasing number of attacks aimed at DNS servers, especially during peak traffic, causes network disruptions and denial of service to legitimate customers. Therefore, ISPs need to take decisive measures to mitigate these threats and safeguard their DNS infrastructure.

One of the main concerns of Conemedia was the number of infected machines run in its networks that were causing security threats and excessive traffic peaks. This concern was amplified by the fact that malware on the infected machines were targeting the DNS servers in the network. At the same time, Conemedia also wanted to take concrete measures against the alarming number of Denial of Service (DoS) attacks on its DNS servers, causing disruptions in the quality of service and leading to customer complaints.

To address these considerations, Conemedia decided to enhance their DNS platform. The goal of the resulting project was to replace their manually managed and unsupported BIND servers with a secure and scalable DNS platform facilitating the monitoring and analysis of DNS traffic; proactive mitigation of threats caused by malware; and automation of the DNS management and provisioning processes.

3. Production Trial

After a thorough evaluation of various DNS solutions offered by leading vendors, Conemedia decided to proceed to a production trial with the Nixu DNS platform due to its advanced threat mitigation model, its DNS monitoring capabilities and overall value. The trial involved two physical x86-based server instances running a dedicated Nixu Secure Name Server (SNS) instance on one and a Nixu NameSurfer Suite instance on another.

Technical Case Study

This case study focuses on the results of the trial conducted during the third quarter of 2011 in Conemedia's production network.

4. Trial Platform

Conemedia installed Nixu NameSurfer Suite Version 7.0.1 and Nixu Secure Name Server (SNS) Version 2.2-1 on two x86-based quad-core CPU servers. Both machines were configured and placed in production network in a major metropolitan area with more than hundred thousand end-users.

Nixu SNS was installed as a DNS server performing both authoritative and recursive functions, with its patent-pending DNS threat mitigation model involving Intrusion Prevention and Rate-Limiting activated. Nixu NameSurfer Suite was configured as the management overlay for the Nixu SNS instance, providing centralized traffic monitoring, DNS management and DNS provisioning capabilities. In order to accommodate Conemedia's performance requirements of 100,000+ queries per second (QPS) per server, two mid-range x86-based rack-mount servers from IBM were selected for the trial.

5. Trial Results

This chapter provides an analysis of the results including logs and traffic information collected by Nixu SNS during the trial period. Any information that would reveal the real identity of Conemedia has been changed or removed for privacy purposes, without affecting the integrity of the data presented.

5.1 DNS Traffic Analysis

The DNS traffic analysis presented in this section is based on the statistics collected by Nixu SNS. The locally collected statistics were automatically pushed to Nixu NameSurfer management overlay for centralised viewing and analysis. A quick look at the results clearly indicates that there is a consistent pattern in the number of queries per second (QPS) served out by Nixu SNS. As indicated by Figures 1-3, the DNS traffic peaked at approximately 3,500 QPS prior to midnight, dropping down to about 250 QPS at 6am. From there, it rapidly rose to slightly above 3,000 QPS by noon, increasing steadily until it reached the peak again at midnight. As represented in Figure 4, Nixu SNS was able to maintain a consistent response time to DNS queries throughout the trial.

While the smooth and predictable DNS traffic patterns depicted in Figures 1-4 are impressive in their own right, they do not reveal the most remarkable result of the trial; namely, Nixu SNS's ability to proactively mitigate the malicious attacks caused by infected clients in the network. Throughout the trial period, the Nixu SNS server instance was targeted with attack attempts and suspect network scans, which would have normally caused irregular traffic peaks. However, as the steady patterns in Figure 1-4 indicate, the Nixu DNS platform was able to successfully thwart these attempts without an impact on the DNS requests from legitimate clients. As far as the quality of service is concerned, a direct outcome of the trial was that DNS-related complaints from customers ceased completely after the DNS server responsible for their network segment was changed to Nixu SNS.

The most remarkable outcome of the whole trial was Nixu SNS's ability to proactively mitigate the malicious malware attacks which caused irregular traffic peak. This was achieved without affecting the DNS requests made by legitimate clients in the network.

Technical Case Study

Figure 1: Graph produced by Nixu NameSurfer Suite showing DNS traffic pattern.

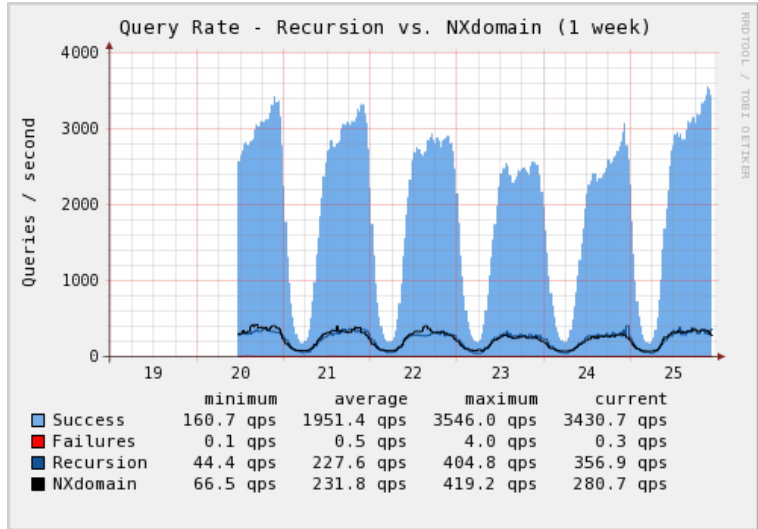


Figure 2: Graph produced by Nixu NameSurfer Suite showing the number of successful queries, which are mostly answered from DNS cache.

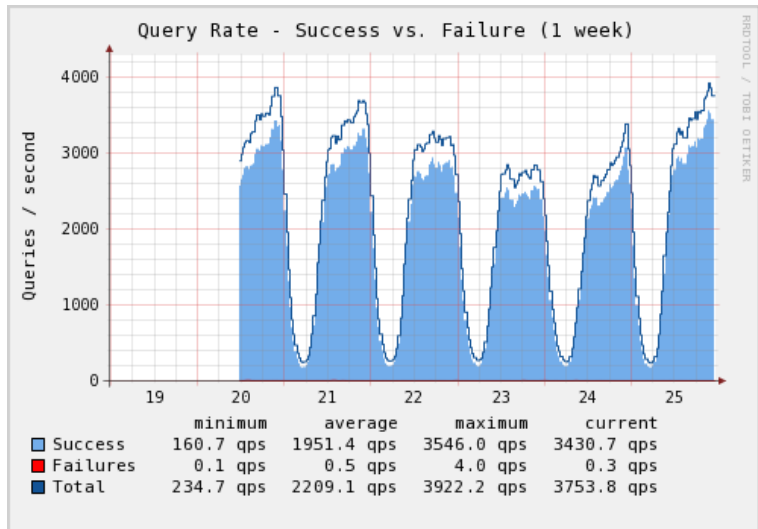
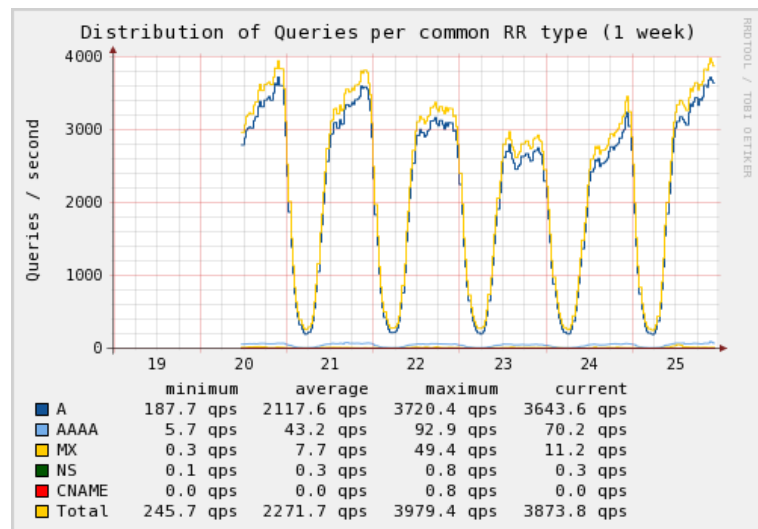
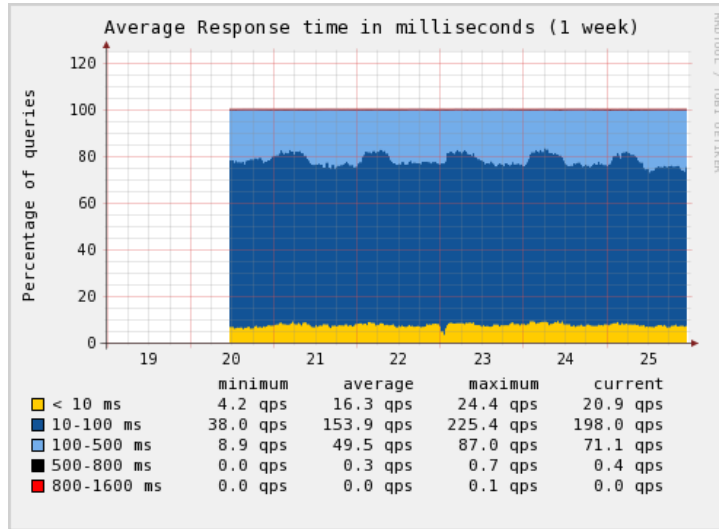


Figure 3: Graph produced by Nixu NameSurfer Suite showing the distribution of DNS queries according to Resource Record (RR) types.



Technical Case Study

Figure 4: Graph produced by Nixu NameSurfer Suite showing DNS server response time in milliseconds.



In addition to DNS traffic statistics, Nixu SNS also collected more detailed information pertaining to DNS traffic. This traffic data was displayed both locally in Nixu SNS and centrally in Nixu NameSurfer management overlay, including information such as:

- the most active zone requests (as shown in Figure 5),
- the most active IP addresses,
- top request sources for DNS queries,
- top resource record (RR) requests made by clients and
- the most requested resource types

Figure 5: The most active zones depicted by Nixu Secure Name Server (SNS).

20 most active zones	Total	Total / sec	Success	Referral	NX RR set	NX domain	Failure
...	96594630	116.7	241396	0	35196	196318038	0
...	23882312	14.2	153156	0	5753	23723403	0
...	3919059	2.3	0	0	0	3919059	0
...	3628776	2.2	0	0	0	3628776	0
...	97645	0.1	0	0	0	97645	0
...	79628	0.0	71749	0	3520	4359	0
...	69473	0.0	65048	0	4425	0	0
...	68642	0.0	67731	0	911	0	0
...	60272	0.0	0	0	0	60272	0
...	17289	0.0	0	0	0	17289	0
...	16053	0.0	0	0	0	16053	0
...	15523	0.0	15198	0	325	0	0
...	12937	0.0	11953	0	984	0	0
...	8563	0.0	5149	0	206	3208	0
...	7332	0.0	0	0	7332	0	0
...	6276	0.0	4026	0	267	1983	0
...	5529	0.0	5529	0	0	0	0
...	5334	0.0	0	0	5334	0	0
...	1250	0.0	1246	0	4	0	0
...	980	0.0	969	0	11	0	0

5.2 Security Related Analysis

In terms of security related findings, an analysis of the log files produced by the Intrusion Prevention System (IPS) included in Nixu SNS revealed the anticipated DoS attacks targeted at Conemedia’s DNS servers. An abnormal number of SYN packets and potentially malign scan attempts were regularly detected by Nixu SNS, prompting the system to place the origin IP addresses into a 3600-second quarantine. Since there were no end-user complaints stemming from the loss of DNS service, it was concluded that:

Technical Case Study

Conemedia was very impressed with the threat mitigation, monitoring and performance characteristics of the Nixu DDI platform.

- the detected attacks were autonomously initiated by malware and therefore did not harm the legitimate use of DNS service; or
- the users that may have knowingly initiated the scan attempts and possible attacks understood why their IP address had been placed into quarantine.

Under both scenarios, placing the IP address into one-hour quarantine was deemed as an appropriate countermeasure, as it facilitated the increase of service level without permanently detaching the infected machines from the DNS service.

In addition to IPS capabilities, Nixu SNS also allows malicious hosts to be partially singled out from DNS service through Rate Limiting. Within this model, the DNS server monitors the amount of DNS traffic originating from an individual IP address, and starts restricting the amount of traffic served if a predefined threshold is breached.

At the beginning of the production trial, the DNS Rate Limiter threshold was set to a relatively loose level of maximum of 500 packets per second per IP address (Figure 6). After an analysis of the pertinent log files, it was detected that no legitimate DNS traffic was blocked at this level, as the highest amount of legitimate traffic from a single IP address was logged at 100 packets per second. Therefore, it was concluded that by setting the DNS Rate Limiter to 200 packets per second, legitimate traffic would always be served out with a sufficient safety margin. In cases where this threshold was breached, Nixu SNS would simply start dropping packets exceeding the threshold, thereby mitigating the attack before it burdened the DNS server process.

Figure 6: The rate limiter settings on Nixu SNS.

Rate limiter

Settings

Service status: **Running** (click buttons to toggle status)

Service start on boot: **Enabled**

Enable statistics: **yes** (Allow rate limiter to collect statistics. Default: no) [View Statistics](#)

Network interface: **any** (The interface to monitor. Default: any)

Threshold Rate: **500** (Packets per seconds. The threshold for limiting incoming traffic.)

Limited Rate: **500** (The limited amount of allowed incoming packets per seconds. Default: 0)

Burst: **1000** (The amount of packets allowed to temporarily exceed the limited rate. Default: 5)

Decay: **100** (The time that the host is being rate-limited/blocked. Default: 900)

Toggle advanced options: **Additional Thresholds** **Excluded IPs**

Save changes **Cancel**

Lastly, based on performance tests carried out using external tools, it was verified that activating or deactivating the DNS Rate Limiting and/or Intrusion Prevention caused no noticeable changes in performance. Coupled with the fact that there were no complaints from affected end-users during the production trial, it was concluded that from the network security perspective, the proactive security measures incorporated into Nixu SNS did not present any downsides in terms of quality of service.

Technical Case Study

6. Conclusions

Regardless of the attacks targeted at Nixu SNS during the production trial, the Nixu DNS platform demonstrated resiliency and satisfactory response times, using no more than 4% or so of its full capacity. This result was largely attributed to the patent-pending proactive security measures incorporated in Nixu SNS which mitigates attacks targeted at the server. It also helps eliminate the need to introduce excessive maximum queries-per-second capacity to safeguard the DNS platform.

Meanwhile, although the production trial was carried out using only one Nixu SNS server instance, it was confirmed that Nixu NameSurfer could be used as the management overlay for up to dozens of individual Nixu SNS server instances. Given the increasing number of DNS queries in service provisioning environments, Conemedia wanted to make sure that they can cost-effectively and easily scale up to upwards of million queries per second in total DNS capacity, providing well-defined upgrade path all the way to the 2020s.

Lastly, since the Nixu SNS server instance was in reality idling away for much of the production trial, it was concluded that even if a healthy safety margin was maintained for future expansion and benign traffic peaks, Conemedia could significantly reduce the number of DNS server instances currently run in its network. Compared to other DNS vendors relying on brute force and excess capacity in mitigating attacks, this approach was deemed to create substantial savings in both Operating Expense (OPEX) and Capital Expense (CAPEX) over the life cycle of the enhanced DNS platform.

About Nixu Software

Nixu Software Oy Ltd is a privately held affiliate of Nixu Group. Headquartered in Helsinki, Finland, and with regional offices in Europe, Americas and Asia Pacific, our mission is to deliver DDI solutions that provide customers with ease of use and piece of mind. Our deliveries are based on a portfolio of virtualization-ready DNS, DHCP and IPAM (DDI) software appliances that support almost any x86-based computing environment, whether virtual or native.

Nixu Software's products have an installed base of more than 3,000 instances worldwide. Our technology is used by hundreds of service providers as well as by dozens of Fortune 500 companies that deem available, reliable and efficiently managed network as a strategic asset.