University of Cincinnati DNSSEC Vendor Analysis

By

Darryl Marsh, Patrick Stasko

Submitted to
the Faculty of the Information Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

University of Cincinnati
College of Applied Science

June 2010

x_________________________      ____________
Darryl Marsh                                                  Date

x__________________________      ____________
Patrick Stasko                                                Date

x__________________________      ____________
John Nyland, Faculty Advisor                       Date
# Table of Contents

Table of Contents ............................................................................................................................ 2

Table of Figures .................................................................................................................................. 4

1. Introduction .................................................................................................................................. 6

2. Project Description and Intended Use .......................................................................................... 7

   2.1 Problem .................................................................................................................................. 7

   2.2 Proposed Solution ..................................................................................................................... 8

      2.2.1 Selected Types .................................................................................................................. 8

      2.2.2 Evaluated Vendors .......................................................................................................... 8

   2.3 User Profile ............................................................................................................................. 9

3. Project Planning ............................................................................................................................. 9

   3.1 Timeline .................................................................................................................................. 9

   3.2 Budget ................................................................................................................................... 10

   3.3 List of Deliverables .................................................................................................................. 12

   3.4 Section of Network ................................................................................................................ 12

4. Risk Management Plan .............................................................................................................. 13

   4.1 Risk 1: Network Anomalies / System Failure ....................................................................... 13

   4.2 Risk 2: Denied access over Firewall ..................................................................................... 14

   4.3 Risk 3: Theft of Equipment .................................................................................................. 14

   4.4 Risk 4: Corruption of Information Store .............................................................................. 14

5. Design Protocols .......................................................................................................................... 15

   5.1 Scorecard ............................................................................................................................... 15

   5.2 Technical Scorecard Items ................................................................................................... 15

   5.3 Business Scorecards Items ................................................................................................. 16

   5.4 Scorecard Analysis .............................................................................................................. 17

6. Testing ........................................................................................................................................ 17

   6.1 BlueCat Networks Configuration ......................................................................................... 19

   6.2 Secure64 Configuration ....................................................................................................... 20

   6.3 Infoblox Configuration ....................................................................................................... 21

7. Proof of Design ............................................................................................................................ 22

   7.1 BlueCat Networks: Scorecard Evaluation ............................................................................. 24
Table of Figures

Figure 1: DNS Attack Vectors........................................................................................................... 7
Figure 2: Timeline........................................................................................................................... 10
Figure 3: Proposed Budget ............................................................................................................. 11
Figure 4: DNS Server Locations.................................................................................................... 13
Figure 5: BlueCat Networks Test Topology ............................................................................... 19
Figure 6: Secure64 Test Topology ............................................................................................... 20
Figure 7: Infoblox Test Topology ............................................................................................... 21
Figure 8: Technical Scorecard ..................................................................................................... 22
Figure 9: Business Scorecard ...................................................................................................... 23
Figure 10: BlueCat Networks Technical Scorecard ................................................................. 24
Figure 11: BlueCat Networks Business Scorecard .................................................................... 25
Figure 12: Secure64 Technical Scorecard .................................................................................. 34
Figure 13: Secure64 Business Scorecard .................................................................................... 35
Figure 14: Infoblox Technical Scorecard .................................................................................... 44
Figure 15: Infoblox Business Scorecard ..................................................................................... 45
Abstract

The University of Cincinnati is an urban, public, research university. The university provides its own domain name system resources. The University’s registrar, EDUCAUSE, is in the process of implementing DNS Security Extensions (DNSSEC) on the .edu root.

The University of Cincinnati DNSSEC Vendor Analysis project aims at testing and analyzing DNSSEC vendor appliances and providing scorecards and a final recommendation to the Office of Information Technologies (UCit) at the University of Cincinnati. The scorecards provide an analysis of technical and business features and the recommendation specifies the highest rated solution in the context of the University’s requirements.
1. Introduction

Domain Name Service (DNS) is a service and a protocol that converts human readable text strings, fully qualified domain names, to IP addresses. DNS is vital to the Internet as it allows the Internet to be fluidly navigable. DNS has been in use since 1983 as a way of making places on the Internet more easily memorable (2). When it was designed, it was done so with scalability, not security, in mind. Nameservers have an innate trust of most information sent to them. Because of this, there are many points where an attacker can replace good information with false information to redirect traffic towards a possibly malicious destination. (Figure 1) These attacks, called DNS cache poisoning attacks, have been common since the mid-1990’s and have enjoyed a recent surge in popularity. In the previous two years, there have been hijackings of the domain names of major banks (9), localized web pages of major search engines, merchandise providers (10), and even the websites of the Internet Corporation for Assigned Names and Numbers (ICANN), who is in charge of the distribution of internet domain names (6).

To help prevent these kinds of attacks, a security solution called DNS Security Extensions (DNSSEC) has been in development for over 10 years. DNSSEC is a set of standards which allow nameservers to ensure that the information received is from an authentic source. That authentication, when it is fully in place, goes all the way back to the root name server that will secure the entire chain of trust. DNSSEC is the solution to securing the existing DNS infrastructure.
2. Project Description and Intended Use

2.1 Problem

Currently, the University of Cincinnati (UC) uses non-secured DNS for all of the domains they own and manage. The top level domain (TLD) registrar for .edu is EDUCAUSE and they have already deployed DNSSEC across their networks. EDUCAUSE currently recommends, but does not require, .edu domain owners to deploy DNSSEC on their DNS zones (6). The amount of momentum behind the deployment of DNSSEC gives UC the opportunity to deploy the security extension, which will help protect UC’s web presence from being compromised. To reach this end, UC will need to arrive at a solution for the best possible hardware, software and support available for the implementation of DNSSEC on their network.
2.2 Proposed Solution

2.2.1 Selected Types

DNSSEC may be implemented in one of four methods. The first, a do-it-yourself solution, utilizes software and hand generating encryption keys. It is best implemented with a setup of a small set of domains. A hybrid approach includes both software and a hardware cryptocard. The use of a cryptocard ensures a secure environment through hardware encryption functions. The third option, an appliance, not only includes the security of generating and storing of keys but also provides enterprise level software encased in automation. Maintenance and technical support are also available from the appliance vendor. Lastly, one may chose to outsource their DNS via a hosted solution. The Office of Information Technologies at the University of Cincinnati (UCit) has stated that an in-house solution, both automated and secure, is required. An appliance is the only possible solution that meets all criteria.

2.2.2 Evaluated Vendors

Three appliance vendors were chosen for final consideration and evaluation. These vendors were BlueCat Networks, Secure64, and Infoblox. The physical equipment was evaluated, from two of the vendors, and a hosted environment, from the third. A fourth vendor, Xelerance, was considered for evaluation, but they were removed from our research as they were unable to provide neither a hosted environment nor a physical appliance for evaluation. These specific vendors were targeted after performing research into DNSSEC and obtaining company profiling information, from ICANN, for currently know DNSSEC vendor solutions.
2.3 User Profile

There are two user profiles for this proposal: administration and network administrators.

Administration is the purchasing power within the University of Cincinnati and the information relevant to administration is located within the business scorecard. The network administrator role will have complete, system-wide access to all data, and will focus on the technical scorecard, of this report, and will contain technical information for the Network Operations Center.

3. Project Planning

3.1 Timeline

In Senior Design I (Autumn), our group completed research on the DNS Security Extension, potential vendors and discussed details regarding the project with UCit Network & Telecom Services. Members of UCit we have corresponded with include: Mark Faulkner, Diane Noelcke, Dave Dessauer, and Bruce Burton. Our group plans to evaluate BlueCat Networks, Secure64 and Infoblox.

In Senior Design II (Winter), each vendor was evaluated and had approximately 15 business days for assessment. This testing was conducted on the University of Cincinnati’s test network, for vendors that shipped their equipment to UC’s datacenter facility. Remote demonstration of products was conducted on the vendor’s network and hardware. Remote configurations allowed greater flexibility due to the lack of time constraints on accessibility of the device.

In Senior Design III (Spring), each vendor’s technical and business scorecards were computed from the appliance’s evaluation, per the specifically drafted criteria. From each score card,
technical and business recommendations were then produced. Finally, a final recommendation was developed from the two individual recommendations.

Our group is confident the structure of the timeline will allow an unbiased testing of each vendor’s hardware. Figure 2 provides details on events that must take place to ensure successful completion.

![Timeline Image](image.png)

Figure 2: Timeline (The timeline shows the steady progression of the project and the accomplishments to follow.)

### 3.2 Budget

The proposed budget is list pricing and does not reflect the price negotiation and special configuration needs. The price of maintenance contracts are based on the specific needs of the
organization through an itemized process and is subject to negotiation. Below is a list of suggested retail pricing for this research.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Qty</th>
<th>Estimated Cost</th>
<th>Project Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infoblox NS-1550A Appliance</td>
<td>Vendor Provided Equipment</td>
<td>2</td>
<td>$16,995</td>
<td>$0</td>
</tr>
<tr>
<td>Secure64 DNS Signer</td>
<td>Vendor Provided Equipment</td>
<td>1</td>
<td>$41,995</td>
<td>$0</td>
</tr>
<tr>
<td>BlueCat Networks Proteus 5000</td>
<td>Vendor Provided Equipment</td>
<td>1</td>
<td>Not Available</td>
<td>$0</td>
</tr>
<tr>
<td>BlueCat Networks Adonis 1000</td>
<td>Vendor Provided Equipment</td>
<td>2</td>
<td>Not Available</td>
<td>$0</td>
</tr>
<tr>
<td>Lenovo Test Laptop</td>
<td>Configuration Hardware</td>
<td>1</td>
<td>$650</td>
<td>$0</td>
</tr>
<tr>
<td>Windows Server 2008 R2 Standard</td>
<td>Test Configuration</td>
<td>1</td>
<td>$1029</td>
<td>$0</td>
</tr>
<tr>
<td>Windows 7 Professional</td>
<td>Test Configuration</td>
<td>1</td>
<td>$300</td>
<td>$0</td>
</tr>
<tr>
<td>Windows Vista Ultimate</td>
<td>Test Configuration</td>
<td>1</td>
<td>$320</td>
<td>$0</td>
</tr>
<tr>
<td>Windows Server 2003 R2 Standard</td>
<td>Test Configuration</td>
<td>1</td>
<td>$999</td>
<td>$0</td>
</tr>
<tr>
<td>Windows XP Professional</td>
<td>Test Configuration</td>
<td>1</td>
<td>$159</td>
<td>$0</td>
</tr>
<tr>
<td>Fedora Core 11 Linux</td>
<td>Test Configuration</td>
<td>1</td>
<td>$0 – GPL</td>
<td>$0</td>
</tr>
<tr>
<td>VMware Workstation 7</td>
<td>Virtualize Test Operating Systems</td>
<td>1</td>
<td>$189</td>
<td>$0</td>
</tr>
<tr>
<td>Labor Hours</td>
<td>Configuration and Test Hours between 3 individuals, actual and projected at $35/hour</td>
<td>250</td>
<td>$8,750</td>
<td>$0</td>
</tr>
</tbody>
</table>

**Total** | **$88,381** | **$0**

Figure 3: Proposed Budget (7, 10, 12, 14, 18, 19, 20, 21) (This budget shows the estimated and actual costs of the hardware and software utilized to complete this project.)
3.3 List of Deliverables

The following is a list of project deliverables:

1) Technical Scorecard
   a) BlueCat Networks
   b) Secure64
   c) Infoblox
   d) Xelerance

2) Business Scorecard
   a) BlueCat Networks
   b) Secure64
   c) Infoblox
   d) Xelerance

3) Recommendation
   a) Business Recommendation
   b) Technical Recommendation
   c) Final Recommendation

* Xelerance declined a product demonstration thus being removed from the evaluation. “At this time we have limited resources in both man power and evaluation units to provide you with [a product demo].” - Sergius Heifa, Xelerance Corporation

3.4 Section of Network

Figure 4 illustrates where the DNS servers are currently located in the University of Cincinnati’s network infrastructure. Figure 4 does not provide detail of the high availability configuration of the server. It provides only a logical view of the infrastructure.
4. Risk Management Plan

4.1 Risk 1: Network Anomalies / System Failure

Risk Contingency Plan: All test equipment has been isolated on its own VLAN and is confined to a single switch on UC’s network.

Risk Worst Case Scenario: To recover from network outage, we would work with UCit’s NOC to identify and resolve the problem.

Project Completion: Upon project completion, this risk will no longer be a threat to the project due to the fact that all of the testing equipment will be offline and will be shipped back to the individual vendors.
4.2 Risk 2: Denied access over Firewall

**Risk Contingency Plan:** All network requirements are discussed and changes requested through UCit’s NOC.

**Risk Worst Case Scenario:** In the event that required access cannot be provided between a firewall, all test equipment can be placed on the same logical network.

**Project Completion:** Upon project completion, this risk will not be an issue due to the fact that network access will no longer be required.

4.3 Risk 3: Theft of Equipment

**Risk Contingency Plan:** To minimize this risk throughout the duration of our project, all equipment will be stored at the University NOC in a locked facility.

**Risk Worst Case Scenario:** In the event that our equipment is stolen, we would work with UCit and the vendor in question to resolve the issue as quickly as possible.

**Project Completion:** Upon project completion, this risk will not be an issue due to the fact that all of the equipment should have been tested and documented before presentations.

4.4 Risk 4: Corruption of Information Store

**Risk Contingency Plan:** To minimize the probability of the corruption of our information store, several backups are made on a daily basis.

**Risk Worst Case Scenario:** In the event that our information store gets corrupted, we would restore the database from one of our backups and continue work.

**Project Completion:** Upon project completion, this risk will still exist as the information from our presentation will come from our information store. To minimize this risk, as
stated before, backups of our data are being made on a daily basis in the event of corruption.

5. Design Protocols

5.1 Scorecard

The vendor analysis portion of the project is addressed through the use of scorecards to evaluate the offerings of the chosen DNSSEC appliances against the requirement of UCit. The scorecards are comprised of grading criteria developed through collaboration with UCit. The technical scorecard evaluates the hardware and security features and compatibility while the business scorecard evaluates the costs and overall value of the appliances.

5.2 Technical Scorecard Items

1. Hardware/Performance Features
   - HA Support (Weight: 5)
   - Gigabit Network Interfaces (Weight: 9)
   - IPv6 Support (Weight: 1)
   - NIST DNSSEC Best Practices (Weight: 9)
   - Automatic Key Rollover (Weight: 5)
   - Emergency Key Rollover (Weight: 9)
   - Syslog support (Weight: 7)
   - Secure Remote Configuration Access (Weight: 9)
   - Rack Mountable (Weight: 1)
   - SNMP Monitoring (Weight: 7)
   - Revert Deployed Changes (Weight: 9)
   - DNS Server Software (Weight: n/a)
2. Security Features

- Internal Firewall (Weight: 9)
- Keys can reside on logically separated network (Weight: 5)
- Hardened OS (Weight: 9)
- Update/Patchable (Weight: 9)
- Keys Encrypted (Weight: 7)
- Whole HDD Encrypted (Weight: 5)
- Local Accounts (Weight: 9)
- No Root Access (Weight: 5)
- Knowledge of Vulnerabilities (Weight: 9)

3. Compatibility

- Compatible with existing infrastructure (Weight: 9)
- Non-DNSSEC enabled devices can read DNSSEC signed answers (Weight: 9)

5.3 Business Scorecards Items

Value/Cost Features

- 5 year Life Cycle/Support (Weight: n/a)
- Warranty (Weight: n/a)
- Vendor Installation Support (Weight: n/a)
- Cost to Implement (Weight: n/a)
- Maintenance Cost (Weight: n/a)
- Product Cost (Weight: n/a)
- Product Lifecycle (Weight: n/a)
- No Outside Purchase Required (Weight: 5)

The second section expands upon the first section and provides a detailed breakdown of each element on the scorecard. The format of the second section is:

- **Scorecard Item Name**: Indicates scorecard criterion.
- **Criteria Explanation**: Detailed explanation of the scorecard criterion and what is desired.
- **Weighted Value**: Assigned weight to the scorecard criterion per the needs of UCit.
- **Vendor Analysis**: Description of how the vendor performed for the criterion.
- **Vendor Response**: Explanation of functionality as stated by the vendor.
- **Final Rating**: Pass or Fail the evaluation for the criterion.
- **Appendix Reference**: Referenced items from the appendix of screen captures and vendor documentation.

### 5.4 Scorecard Analysis

The technical analysis comprised of running each appliance through various technical scenarios and tests. The business analysis was devised and documented through the scorecard that had been drafted between the project team and UCit, for the purposes of this project. Both analyses include a criterion weighting system in which a vendor is selected that best matches the technical and business needs that UCit has established.

### 6. Testing

Configuration of the DNSSEC test appliances can be configured in various high availability configurations. Testing for each vendor is slightly different because of the vendor’s specific management interfaces. The end result of each appliance is to provide DNSSEC signed DNS records to an external network. Testing will indicate that each vendor can successfully deploy DNSSEC, in accordance with current DNSSEC industry standards and best practices. Each vendor is setup differently based on a variety of factors such as, but not limited to, recommended topology configuration of each set of appliances and if testing is performed remotely or in-house. Vendors that physically supply their product to the Network Operations Center will be
configured in UC’s Demilitarized Zone (DMZ) which is a portion of the network which is accessible by external networks, with an emphasis on security. Four public IP address have been made available for this proposal and two of them have inbound TCP and UDP DNS traffic (port 53) allowed to pass through the DMZ’s external firewall. The IP’s that have been reserved for use are 129.137.254.200 - 129.137.254.203. Port 53 TCP, UDP and ping connections have been passed through the firewall on the following IP addresses: 129.137.254.202 and 129.137.254.203. Once the configuration is successfully, each server will be tested to perform queries from an external host using Dig, a Linux DNS query tool that provides extended information. Dig supports DNS as well as DNSSEC.

Remote configurations will enable faster testing as the appliance is already deployed and allows research to focus on the vendor’s claims instead of the initial configuration. The configuration will be provided by the vendor for remote demonstrations.
6.1 BlueCat Networks Configuration

Figure 5: BlueCat Networks Test Topology (This illustration shows the network topology of the BlueCat Networks appliances which include two Adonises and one Proteus.)

Basic Setup Information

Appliance Models:
- Proteus: PROTEUS-5000HS-221
- Adonis 1: ADONIS-1000HS-511
- Adonis 2: ADONIS-1000HS-511

Addressing:
- Proteus: 129.137.254.201 (VLAN 36)
- Adonis 1: 129.137.254.202 (VLAN 36)
- Adonis 2: 129.137.254.203 (VLAN 36)
- Gateway: 129.137.254.1 (VLAN 36)

DNS Entries:
- adonis1.junkbucket.org
- adonis2.junkbucket.org
6.2 Secure64 Configuration

Figure 6: Secure64 Test Topology (This illustration shows the network topology of the Secure64 signer which is logically placed between the primary DNS server and Hidden Master.)

Basic Setup Information

Appliance Model:
- Secure64 Signer: Secure64 Signer

Addressing:
- noco216.secure64.com

DNS Entries:
- secure64.junkbucket.org
6.3 Infoblox Configuration

Figure 7: Infoblox Test Topology (This illustration shows the network topology of the primary and secondary Infoblox appliances.)

Basic Setup Information

Appliance Models:
- 1550 Series: Infoblox-1550-A
- 1550 Series: Infoblox-1550-A

Addressing:
- Infoblox 1: 129.137.254.202 (VLAN 36)
- Infoblox 2: 129.137.254.203 (VLAN 36)
- Gateway: 129.137.254.1 (VLAN 36)

DNS Entries:
- infoblox.junkbucket.org
- infoblox2.junkbucket.org
### 7. Proof of Design

#### Technical Scorecard Evaluation

<table>
<thead>
<tr>
<th>DNSSEC Signer Requirements</th>
<th>Weighted Value</th>
<th>BlueCat</th>
<th>Secure64</th>
<th>Infoblox</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HA Support</td>
<td>5</td>
<td>🟡</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Gigabit Network Interfaces</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>IPv6 Support</td>
<td>1</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>NIST DNSSEC Best Practices</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Automatic Key Rollover</td>
<td>5</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Emergency Key Rollover</td>
<td>5</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Syslog Support</td>
<td>7</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Secure Remote Configuration Access</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>1</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>SNMP Monitoring</td>
<td>7</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Revertible Deployed Changes</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>DNS Server Software Not Weighted</td>
<td>Not Weighted</td>
<td>BIND</td>
<td>NSD</td>
<td>BIND</td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Firewall</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Keys can reside on logically seperated network</td>
<td>5</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Hardended OS</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Update/Patchable</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Keys Encrypted</td>
<td>7</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Whole HDD Encrypted</td>
<td>5</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Local Account Access</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>No Root Access</td>
<td>5</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Knowledge of Vulnerabilities</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td><strong>Compatibility</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compatible with existing infrastructure</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Non-DNSSEC enabled devices can read DNSSEC signed answers</td>
<td>9</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>156</td>
<td>139</td>
<td>137</td>
<td>151</td>
</tr>
</tbody>
</table>

Figure 8: Technical Scorecard (This illustration shows the technical criteria used to evaluate each vendor.)
## Business Scorecard Evaluation

<table>
<thead>
<tr>
<th>DNSSEC Signer Requirements</th>
<th>Weighted Value</th>
<th>BlueCat</th>
<th>Secure64</th>
<th>Infoblox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value/Cost Feature</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Year Life Cycle/Support</td>
<td>Not Weighted</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Warranty</td>
<td>Not Weighted</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Vendor Installation Support</td>
<td>Not Weighted</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cost to implement</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>Maintenance Cost</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>Product Cost</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>Product Lifecycle</td>
<td>Not Weighted</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No Outside Purchase Required</td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total

<table>
<thead>
<tr>
<th></th>
<th>BlueCat</th>
<th>Secure64</th>
<th>Infoblox</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 9: Business Scorecard (This illustration shows the business criteria used to evaluate each vendor.)
### 7.1 BlueCat Networks: Scorecard Evaluation

<table>
<thead>
<tr>
<th>DNSSEC Signer Requirements</th>
<th>Weighted Value</th>
<th>BlueCat</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HA Support</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Gigabit Network Interfaces</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>IPv6 Support</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>NIST DNSSEC Best Practices</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Automatic Key Rollover</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Emergency Key Rollover</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Syslog Support</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Secure Remote Configuration Access</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>SNMP Monitoring</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Revertible Deployed Changes</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>DNS Server Software</td>
<td>Not Weighted</td>
<td>BIND</td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Firewall</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Keys can reside on logically seperated network</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Hardended OS</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Update/Patchable</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Keys Encrypted</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Whole HDD Encrypted</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Local Account Access</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>No Root Access</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Knowledge of Vulnerabilities</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td><strong>Compatibility</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compatible with existing infrastructure</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Non-DNSSEC enabled devices can read DNSSEC signed answers</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>156</td>
<td>139</td>
</tr>
</tbody>
</table>

Figure 10: BlueCat Networks Technical Scorecard (This illustration shows the technical evaluation of BlueCat Networks.)
### DNSSEC Signer Requirements

<table>
<thead>
<tr>
<th>Value/Cost Feature</th>
<th>Weighted Value</th>
<th>BlueCat</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Year Leife Cycle/Support</td>
<td>Not Weighted</td>
<td>Yes</td>
</tr>
<tr>
<td>Warranty</td>
<td>Not Weighted</td>
<td>Yes</td>
</tr>
<tr>
<td>Vendor Installation Support</td>
<td>Not Weighted</td>
<td>Yes</td>
</tr>
<tr>
<td>Cost to implement</td>
<td>Not Weighted</td>
<td>TBD</td>
</tr>
<tr>
<td>Maintenance Cost</td>
<td>Not Weighted</td>
<td>TBD</td>
</tr>
<tr>
<td>Product Cost</td>
<td>Not Weighted</td>
<td>TBD</td>
</tr>
<tr>
<td>Product Lifecycle</td>
<td>Not Weighted</td>
<td>Yes</td>
</tr>
<tr>
<td>No Outside Purchase Required</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>5</strong></td>
<td><strong>5</strong></td>
</tr>
</tbody>
</table>

Figure 11: BlueCat Networks Business Scorecard (This illustration shows the business evaluation of BlueCat Networks.)

### 7.2 BlueCat Networks: Scorecard Detailed Analysis

#### 1. Hardware/Performance Features

**HA Support**

**Criterion Explanation:** This criterion denotes that the appliance is capable of syncing with one or more like appliances. If one of the appliances should malfunction, the services offered should be maintained with little or no disruption.

**Weighted Value:** 5

**Vendor Analysis:** BlueCat Networks Adonis supports active/passive architecture.

**Vendor Response:** The Adonis HA solution utilizes two servers in an active – passive cluster configuration. The two servers share an address that clients use to perform queries against. The servers are connected using a heartbeat signal to determine the health of the active server. In the event that the active server fails, control is passed to the passive server which then takes on the active role.

**Final Rating:** Pass

**Appendix References:** Appendix A: Figure 1, p. 6 - BCN_XHA_for_DNS_and_DHCP.pdf

**Gigabit Network Interfaces**
Criterion Explanation: This criterion denotes that the appliance’s Ethernet ports support transmitting Ethernet frames at a rate of a gigabit per second, as defined by the IEEE 802.3-2008 standard.

Weighted Value: 9

Vendor Analysis: The BlueCat Networks ADONIS-1000HS-511 appliances are capable of transmission of Ethernet frames at both 100mbps and 1000mbps.

Vendor Response: The Adonis-1000 provides two gigabit Ethernet interfaces – 10/100/1000Base-T Ethernet, Auto-sensing link speed.

Final Rating: Pass

IPv6 Support

Criterion Explanation: This criterion denotes that the appliance is capable of operating in an IPv6 addressing scheme.

Weighted Value: 1

Vendor Analysis: The BlueCat Networks Proteus appliance has the functionality to support IPv6 DNS hosts.

Vendor Response: Mainstream support for IPv6 is included in Proteus version 3.0.2.

Final Rating: Pass

Appendix References: Appendix A: Figure 2 - 3

NIST DNSSEC Best Practices

Criterion Explanation: This criterion denotes that the appliance is capable of implementing all required NIST DNSSEC Best Practice Guidelines.

Weighted Value: 9

Vendor Analysis: The BlueCat Networks Proteus and Adonis implement all required NIST DNSSEC Best Practice Guidelines.

Vendor Response: BlueCat’s products can ease the burden of implementing and administering DNSSEC, as well as address all other DNS security requirements outlined in the NIST Special Publication 800-81r1.

Final Rating: Pass

Appendix References: p. 15 - wp_dnssec.pdf

Automatic Key Rollover
**Criterion Explanation:** This criterion denotes that the appliance is capable of exchanging expired key signing keys and zone signing keys with new pre-published keys.

**Weighted Value:** 5

**Vendor Analysis:** The BlueCat Networks Proteus supports scheduling automatic rollovers for both ZSK and KSK. The Proteus supports notification via an SNMP or email of soon to expire keys.

**Vendor Response:** An administrator can configure a scheduled rollover period for both the ZSK and the KSK from a DNSSEC signing policy.

**Final Rating:** Pass

**Appendix References:** Appendix A: Figure 4, p. 13 - wp_dnssec.pdf

---

**Emergency Key Rollover**

**Criterion Explanation:** This criterion denotes that the appliance permits administrators to manually exchange key signing keys and zone signing keys with new keys that have are not currently published.

**Weighted Value:** 9

**Vendor Analysis:** The BlueCat Networks Proteus supports the manual signing of keys without the requirement of a secondary key being published.

**Vendor Response:** BlueCat supports double signing for keys, an administrator has the ability to create a backup set of keys that are always available.

**Final Rating:** Pass

**Appendix References:** Appendix A: Figure 5

---

**Syslog Support**

**Criterion Explanation:** This criterion denotes that the appliance is capable of exporting generated logs to a Syslog server.

**Weighted Value:** 7

**Vendor Analysis:** The BlueCat Networks Proteus supports Syslog redirection for none, one or multiple Syslog servers with individual log selection.

**Vendor Response:** Proteus supports Syslog redirection via the Syslog service daemon that allows multiple redirection destinations and redirection selectors.

**Final Rating:** Pass

**Appendix References:** Appendix A: Figure 6, p. 368 - Proteus_Administration_Guide_3.0.2.pdf
Secure Remote Configuration Access

**Criterion Explanation:** This criterion denotes that the appliance provides configuration access via either SSH or a web interface encrypted by an SSL or TLS connection.

**Weighted Value:** 9

**Vendor Analysis:** The BlueCat Networks Proteus supports both HTTP over SSL and SSH. SSH is enabled by default while HTTPS is disabled by default. The BlueCat Networks Adonis supports SSH which is enabled by default.

**Vendor Response:** The Proteus server has SSH2 connectivity enabled by default on all except military models. However, the Administration Console offers the ability to enable and disable SSH connectivity. HTTPS support configuration mode allows users to configure Proteus HTTPS support for the management console. Secure Shell (SSH) Version 2 allows a client to communicate with the Adonis and access the Administration Console remotely.

**Final Rating:** Pass

**Appendix References:** Appendix A: Figures 7 - 9, p. 75 - Protus_Admin_Manual.pdf, p. 361 - Proteus_Administration_Guide_3.0.2.pdf, p. 51 - Adonis_Administration_6.0.2.pdf

Rack Mountable

**Criterion Explanation:** This criterion denotes that the appliance is equipped with proper hardware to be mounted in an equipment rack.

**Weighted Value:** 1

**Vendor Analysis:** The BlueCat Networks Proteus and Adonis both ship with sliding rails that are rack mountable. Depending on what type of rack the Adonis is installed, the sliding rails may not be necessary.

**Vendor Response:** Both the Proteus and Adonis support installation in a standard and telco-style rack.

**Final Rating:** Pass

**Appendix References:** Appendix A: Figure 10, p. 10 - Adonis_Installation_Guide_6.0.2.pdf, p. 12 - Proteus_Quick_Start_guide_3.0.2.pdf

SNMP Monitoring

**Criterion Explanation:** This criterion denotes that the appliance is capable of acting as a SNMP agent.

**Weighted Value:** 7
Vendor Analysis: The BlueCat Networks Proteus supports the following SNMP parameters: Host, Version, Port Number, Username, Security Level, Authentication Type, Auth Passphrase and Privacy Passphrase.

Vendor Response: Proteus includes support for SNMP versions 1, 2c, and 3. By default, SNMP version 2c is configured but is not enabled.

Final Rating: Pass

Appendix References: Appendix A: Figure 11, p. 370 - Proteus_Administration_Guide_3.0.2.pdf

Revertible Deployed Changes

Criterion Explanation: This criterion denotes that the appliance permits administrators to revert running configurations to a previous configuration state.

Weighted Value: 9

Vendor Analysis: While evaluating the Proteus, the revert transaction feature did not complete successfully when attempting to revert a ZSK rollover.

Vendor Response: The BlueCat Networks Proteus supports the reversing of individual transactions.

Final Rating: Fail

Appendix References: Appendix A: Figure 12, p. 105 - Proteus Admin Guide.pdf

DNS Server Software

Criterion Explanation: This criterion describes the DNS server software running on the appliance.

Weighted Value: Not Weighted

Vendor Analysis: The BlueCat Networks Adonis operates off of a customized version of BIND.

Vendor Response: None

Final Rating: N/A

2. Security Features

Internal Firewall

Criterion Explanation: This criterion denotes that the appliance supports a self-regulating firewall.
**Vendor Analysis:** The Adonis and Proteus appliances only had open ports for the services that were running, at the moment of testing.

**Vendor Response:** An Adonis appliance operates with very few open ports; it uses an encrypted control port to connect to the Management Console on the administrator’s PC. Ports are opened only if they are required for the project being deployed on the appliance. Operating behind a dynamically configured packet-filtering firewall, the Adonis appliance is well suited to network conditions anywhere including hostile environments such as DMZs or the Internet.

**Final Rating:** Pass

**Appendix References:** p. 11 - Adonis_Administration_6.0.2.pdf

---

**Keys can reside on logically separated network**

**Criterion Explanation:** This criterion denotes that the appliance has the capability of storing its Key Signing Keys and Zone Signing Keys and that the appliance is not required to be publically facing.

**Weighted Value:** 5

**Vendor Analysis:** The DNSSEC keys are stored on the Adonis appliance. This appliance does not have to be publically facing, in order for DNS to be operational, if a hidden master configuration is utilized.

**Vendor Response:** None

**Final Rating:** Pass

**Appendix References:** pp. 11-12 - Adonis_Administration_6.0.2.pdf

---

**Hardened OS**

**Criterion Explanation:** This criterion denotes that the appliance’s operating system has measures in place to reduce the likelihood of being compromised.

**Weighted Value:** 9

**Vendor Analysis:** None

**Vendor Response:** BlueCat Network’s Linux™-based operating system is stripped down to its essential code, so the kernel does not load new modules during runtime. The DNS daemon (service) also runs in a chroot jailed environment to prevent the server from being compromised in the highly unlikely event that the service is breached.

**Final Rating:** Conditional Pass

**Appendix References:** pp. 11-12 - Adonis_Administration_6.0.2.pdf
**Update/Patchable**

**Criterion Explanation:** This criterion denotes that the appliance is capable of updating its code base.

**Weighted Value:** 9

**Vendor Analysis:** The Proteus can be updated via a manual upload or a streaming web download, capable of communicating through a web or TCP proxy. The Adonis may be updated from a push from the Proteus or may be updated via a manual upload or a streaming web download, capable of communicating through a web or TCP proxy.

**Vendor Response:** Updates to the software and operating system are completely automated and encrypted thanks to the known hardware and software combinations implicit with appliances.

**Final Rating:** Pass

**Appendix References:** Appendix A: Figures 13 - 15

**Keys Encrypted**

**Criterion Explanation:** This criterion denotes that the appliance is capable of encrypting its Key Signing Keys and Zone Signing Keys via the means of software or hardware encryption.

**Weighted Value:** 7

**Vendor Analysis:** The BlueCat Networks Adonis does not encrypt either the KSK or ZSK.

**Vendor Response:** All keys on the Adonis server are stored in a restricted area within the jailed DNS environment.

**Final Rating:** Fail

**Appendix References:** p. 9 - wp_dnssec.pdf

**Whole HDD Encrypted**

**Criterion Explanation:** This criterion denotes that the appliance is capable of fully encrypting its hard drive(s) with the exception of the master boot record.

**Weighted Value:** 5

**Vendor Analysis:** The BlueCat Networks Proteus and Adonis do not support full disk encryption.

**Vendor Response:** None

**Final Rating:** Fail
Local Account Access

**Criterion Explanation:** This criterion denotes that the appliance allows local accounts and that granular permissions may be provisioned.

**Weighted Value:** 9

**Vendor Analysis:** The Proteus supports the creation of local accounts including that of administrator and users with select granular access.

**Vendor Response:** An administrator can assign a user or a group default access rights. Proteus supports mixed-mode authentication through local, RADIUS, LDAP, Microsoft Active Directory or Kerberos. Support for RSA Secure ID is accomplished through the RADIUS authentication module.

**Final Rating:** Pass

**Appendix References:** p. 100 & p. 106 - Proteus_Administrator_Guide_3.0.2.pdf

No Root Access

**Criterion Explanation:** This criterion denotes that the appliance does not support the functionality of a root user account.

**Weighted Value:** 5

**Vendor Analysis:** Both the Proteus and Adonis support root user accounts via consol and SSH.

**Vendor Response:** None

**Final Rating:** Fail

Knowledge of Vulnerabilities

**Criterion Explanation:** This criterion denotes that the appliance vendor has prior knowledge of security risks before they are announced to the public.

**Weighted Value:** 9

**Vendor Analysis:** BlueCat Networks is both a CERT advisory participant and Patron member of ISC.

**Vendor Response:** BlueCat Networks is a participant in the CERT advisory notifications, whereby BlueCat is notified of any potential security risk to the applications and programs running on the system in advance of their public release. This gives BlueCat Networks advanced notification of any impending security risk, providing BlueCat with enough time to address or mitigate the security risk. As a Patron member of ISC, BlueCat Networks receives advanced notification of all software updates and security patches. Customers benefit from this relationship, as BlueCat Networks is able to update software and address security vulnerabilities before they are announced to the public.
3. Compatibility

Compatible with Existing Infrastructure

**Criterion Explanation:** This criterion denotes that the appliance is capable of being installed as a DNSSEC signer in the University of Cincinnati’s planned DNS configuration.

**Weighted Value:** 9

**Vendor Analysis:** The BlueCat Networks Adonis is not meant to be used as a stand-alone DNSSEC signer, but as an appliance that provides DNS services with DNSSEC enabled. For the Adonis to be implemented, the University’s current DNS architecture would be entirely restructured.

**Vendor Response:** None

**Final Rating:** Pass

Non-DNSSEC enabled devices can read DNSSEC signed answers

**Criterion Explanation:** This criterion denotes that non-DNSSEC enabled devices are capable of reading DNSSEC signed DNS responses that are signed by the appliance.

**Weighted Value:** 9

**Vendor Analysis:** A non-DNSSEC enabled client was able to read the DNS zone data that is signed by the BlueCat Networks Adonis.

**Vendor Response:** None

**Final Rating:** Pass
### 7.3 Secure64: Scorecard Evaluation

<table>
<thead>
<tr>
<th>DNSSEC Signer Requirements</th>
<th>Weighted Value</th>
<th>Secure64</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HA Support</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Gigabit Network Interfaces</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>IPv6 Support</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>NIST DNSSEC Best Practices</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Automatic Key Rollover</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Emergency Key Rollover</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Syslog Support</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Secure Remote Configuration Access</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>SNMP Monitoring</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Revertible Deployed Changes</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>DNS Server Software</td>
<td>Not Weighted</td>
<td>NSD</td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Firewall</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Keys can reside on logically separated network</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Hardended OS</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Update/Patchable</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Keys Encrypted</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Whole HDD Encrypted</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Local Account Access</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>No Root Access</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Knowledge of Vulnerabilities</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td><strong>Compatibility</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compatible with existing infrastructure</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Non-DNSSEC enabled devices can read DNSSEC signed answers</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>156</td>
<td>137</td>
</tr>
</tbody>
</table>

Figure 12: Secure64 Technical Scorecard (This illustration shows the technical evaluation of Secure64.)
7.4 Secure64: Scorecard Detailed Analysis

1. Hardware/Performance Features

**HA Support**

**Criterion Explanation:** This criterion denotes that the appliance is capable of syncing with one or more like appliances. If one of the appliances should malfunction, the services offered should be maintained with little or no disruption.

**Weighted Value:** 5

**Vendor Analysis:** The Secure64 Signer is only capable of operating in a single appliance configuration.

**Vendor Response:** The Secure64 Signer is capable of Primary and Secondary DNS server roles but does not provide active-active or active-passive high availability configurations. There are no clustering options available.

**Final Rating:** Fail

**Gigabit Network Interfaces**

**Criterion Explanation:** This criterion denotes that the appliance’s Ethernet ports support transmitting Ethernet frames at a rate of a gigabit per second, as defined by the IEEE 802.3-2008 standard.

**Weighted Value:** 9
**Vendor Analysis:** Secure64 Signer is intended to be with a recommended HP Integrity rx2660 server. The HP Integrity rx2660 is capable of transmission of Ethernet frames at 10/100/1000mbps.

**Vendor Response:** The HP Integrity rx2660 server provides two gigabit Ethernet interfaces capable of half and full duplex at speeds of 10/100/1000mbps auto sensing link speeds.

**Final Rating:** Pass

**Appendix References:** p. 2 - Secure64 DNS Signer - datasheet.pdf

---

**IPv6 Support**

**Criterion Explanation:** This criterion denotes that the appliance is capable of operating in an IPv6 addressing scheme.

**Weighted Value:** 1

**Vendor Analysis:** The Secure64 Signer supports protocols for IPv6 DNS hosts.

**Vendor Response:** The Secure64 Signer is IPv6 Ready Phase-2 Certified which covers over 450 tests to validate IPv6 connectivity.

**Final Rating:** Pass

**Appendix References:** p. 4 - Secure64Signer_v3.1.8_adminguide.pdf

---

**NIST DNSSEC Best Practices**

**Criterion Explanation:** This criterion denotes that the appliance is capable of implementing all required NIST DNSSEC Best Practice Guidelines.

**Weighted Value:** 9

**Vendor Analysis:** The Secure64 Signer implements all required NIST DNSSEC Best Practice Guidelines.

**Vendor Response:** The Secure64 Signer by default has values which are in line with that of the NIST DNSSEC recommended guidelines for an ideal implementation of DNSSEC.

**Final Rating:** Pass

**Appendix References:** pp. 45,55,59,82 - Secure64Signer_v3.1.8_adminguide.pdf

---

**Automatic Key Rollover**

**Criterion Explanation:** This criterion denotes that the appliance is capable of exchanging expired key signing keys and zone signing keys with new pre-published keys.
**Weighted Value:** 1

**Vendor Analysis:** The Secure64 Signer can operate in automatic mode which exchanges expired keys with new pre-published keys.

**Vendor Response:** The Secure64 Signer will resign keys on scheduled rollover events as defined by “dnssec-zsk-rollover <crontab>“.

**Final Rating:** Pass

**Appendix References:** p. 56 - Secure64Signer_v3.1.8_adminguide.pdf

---

**Emergency Key Rollover**

**Criterion Explanation:** This criterion denotes that the appliance permits administrators to manually exchange key signing keys and zone signing keys with new keys that have not currently published.

**Weighted Value:** 9

**Vendor Analysis:** The Secure64 Signer supports manual key rollover allowing administrator to override any automatic settings in the event of an emergency without the pre-published key timeframe.

**Vendor Response:** The Secure64 Signer supports emergency key rollover by issuing a manual key rollover by the following command “dnssec rollkey <zone>” from the authdnsadmin privileged user CLI.

**Final Rating:** Pass

**Appendix Reference:** p. 56 - Secure64Signer_v3.1.8_adminguide.pdf

---

**Syslog Support**

**Criterion Explanation:** This criterion denotes that the appliance is capable of exporting generated logs to a Syslog server.

**Weighted Value:** 7

**Vendor Analysis:** Secure64 Signer is able to communicate information and diagnostics logs to a Syslog server.

**Vendor Response:** Secure64 Signer is built with Syslog support; the ability to configure a remote Syslog server is optional. All log entries are stored in a local Syslog daemon by default. Signer automatically generates notifications for all signing and key management events (including normal, warning and error events), using syslog alerts, SNMP traps.

**Final Rating:** Pass
Secure Remote Configuration Access

**Criterion Explanation:** This criterion denotes that the appliance provides configuration access via either SSH or a web interface encrypted by an SSL or TLS connection.

**Weighted Value:** 9

**Vendor Analysis:** The Secure64 Signer provides secure remote configuration via SSH or a web interface which are secured using SSL or TLS technologies.

**Vendor Response:** The Secure64 Signer provides SSH v2 secure remote access only. SSH v2 uses AES based encryption for secure transport of remote configuration data.

**Final Rating:** Pass

Rack Mountable

**Criterion Explanation:** This criterion denotes that the appliance is equipped with proper hardware to be mounted in an equipment rack.

**Weighted Value:** 1

**Vendor Analysis:** The Secure64 Signer form factor is designed to be mounted in an equipment rack commonly found in computer data centers.

**Vendor Response:** The recommended hardware usage with the Secure64 software is the HP Integrity rx2660. The HP Integrity rx2660 is a 2U rack mount form factor.

**Final Rating:** Pass


SNMP Monitoring

**Criterion Explanation:** This criterion denotes that the appliance is capable of acting as a SNMP agent.

**Weighted Value:** 7

**Vendor Analysis:** The Secure64 Signer is capable of the role of an SNMP agent to transmit configurations remotely.

**Vendor Response:** Signer automatically generates notifications for all signing and key management events (including normal, warning and error events), using syslog alerts, SNMP traps.
Final Rating: Pass

Appendix References: p. 2 - Secure64 DNS Signer - datasheet.pdf

Revertible Deployed Changes

Criterion Explanation: This criterion denotes that the appliance permits administrators to revert running configurations to a previous configuration state.

Weighted Value: 9

Vendor Analysis: The Secure64 Signer has the ability to revert to previously configuration states.

Vendor Response: The Secure64 Signer has built-in backup and restore the entire system but not individual revertible running configurations based on zones.

Final Rating: Fail

DNS Server Software

Criterion Explanation: This criterion describes the DNS server software running on the appliance.

Weighted Value: Not Weighted

Vendor Analysis: Secure64 Signer DNS server software is based off a public open source project.

Vendor Response: Secure64 Signer is Name Server Daemon (NSD) based.

Final Rating: N/A

2. Security Features

Internal Firewall

Criterion Explanation: This criterion denotes that the appliance supports a self-regulating firewall.

Weighted Value: 9

Vendor Analysis: The Secure64 Signer does disregard incoming traffic on ports that are not required for the currently running configuration’s operation.

Vendor Response: The Secure64 signer disregards incoming traffic on all ports other than the ports configured for DNS queries (TCP and UDP port 53), SSH (TCP port 22), and BGP (TCP port 179) if configured. Rate-limiting and Mitigation rules are also available for the ports that are exposed to decrease the risk of data floods.
Final Rating: Pass

Keys can reside on logically separated network

Criterion Explanation: This criterion denotes that the appliance has the capability of storing its Key Signing Keys and Zone Signing Keys and that the appliance is not required to be publically facing.

Weighted Value: 5

Vendor Analysis: The Secure65 Signer is to be configured such that the signed records are to be passed onto DNS master and slave servers, but the Signer itself is not to be publically facing.

Vendor Response: None

Final Rating: Pass

Appendix References: pg. 2 Secure64 DNS Signer - datasheet.pdf

Hardened OS

Criterion Explanation: This criterion denotes that the appliance’s operating system has measures in place to reduce the likelihood of being compromised.

Weighted Value: 9

Vendor Analysis: None

Vendor Response: The Secure64 Signer depends on the Implementation of the Trusted Platform Module (TPM) chip in the HP rx2660 server. The Secure64 Signer is a Genuine Micro Operating System which segments running processes in a secure container in memory.

Final Rating: Conditional Pass

Update/Patchable

Criterion Explanation: This criterion denotes that the appliance is capable of updating its code base.

Weighted Value: 9

Vendor Analysis: The Secure64 Signer is updatable with both patches and operating system updates.

Vendor Response: The Secure64 Signer is updatable and downloads can be obtained through https://download.secure64.com. Each update must be manually transferred to the signer and does not directly download the updates from the internet.

Final Rating: Pass
Appendix References: p. 120 - Secure64Signer_v3.1.8_adminguide.pdf

**Keys Encrypted**

**Criterion Explanation:** This criterion denotes that the appliance is capable of encrypting its Key Signing Keys and Zone Signing Keys via the means of software or hardware encryption.

**Weighted Value:** 7

**Vendor Analysis:** The Secure64 Signer encrypts private keys by encryption.

**Vendor Response:** Private Keys are encrypted through the TPM chip which is a hardware based encryption for maximum security.

**Final Rating:** Pass

Appendix References: p. 10 - Secure64Signer_v3.1.8_adminguide.pdf

**Whole HDD Encrypted**

**Criterion Explanation:** This criterion denotes that the appliance is capable of fully encrypting its hard drive(s) with the exception of the master boot record.

**Weighted Value:** 5

**Vendor Analysis:** The Secure64 Signer encrypts some, but not all of its hard drive contents.

**Vendor Response:** SourceT Micro OS encrypts and provides integrity checks for critical, non-public information, using symmetric keys generated when the file system partition is defined. The keys are retained securely across system shutdown and reboot.

**Final Rating:** Fail

Appendix References: pg. 10 Secure64Signer_v3.1.8_adminguide.pdf

**Local Account Access**

**Criterion Explanation:** This criterion denotes that the appliance allows local accounts and that granular permissions may be provisioned.

**Weighted Value:** 9

**Vendor Analysis:** The Secure64 Signer supports local accounts and provides granular permissions for local accounts.

**Vendor Response:** The Secure64 Signer supports local accounts and have granular level of permissions which are broken up into various levels as follows: sysadmin, authdnsadmin, bgpadmin, loginadmin, securityadmin and upgrade modes.
Final Rating: Pass

Appendix References: p. 1 - Secure64Signer_command_reference.pdf

No Root Access

Criterion Explanation: This criterion denotes that the appliance does not support the functionality of a root user account.

Weighted Value: 5

Vendor Analysis: The Secure64 Signer does not support root accounts. Users are contained to a limited subset of function they can perform based upon their account access role.

Vendor Response: The Secure64 Signer does not provide full root access to the device. There are a multitude of user levels which are proprietary to Secure64’s Command Line Interface (CLI).

Final Rating: Pass

Knowledge of Vulnerabilities

Criterion Explanation: This criterion denotes that the appliance vendor has prior knowledge of security risks before they are announced to the public.

Weighted Value: 9

Vendor Analysis: Secure64 is notified of potentially effecting vulnerabilities by CERT.

Vendor Response: Secure64 is not an Advisory Participant with CERT but does receive notification of potentially effecting vulnerabilities via secured email. The vulnerability is not publically announced until all potentially effected vendors report back that they have a resolution to the patch.

Final Rating: Pass

3. Compatibility

Compatible with Existing Infrastructure

Criterion Explanation: This criterion denotes that the appliance is capable of being installed as a DNSSEC signer in the University of Cincinnati’s planned DNS configuration.

Weighted Value: 9

Vendor Analysis: The Secure64 Signer can work in pass-through mode which only signs DNS records and passes them to existing DNS servers for distribution.
Vendor Response: The Secure64 Signer works in pass-through mode and passes signed DNSSEC DNS records to other vendor’s DNS server software such as BIND, Microsoft DNS and NSD.

Final Rating: Pass

Appendix References: p. 1 - Secure64 DNS Signer - datasheet.pdf

Non-DNSSEC enabled devices can read DNSSEC signed answers

Criterion Explanation: This criterion denotes that non-DNSSEC enabled devices are capable of reading DNSSEC signed DNS responses that are signed by the appliance.

Weighted Value: 9

Vendor Analysis: A non-DNSSEC enabled client was able to read the DNS zone data that is signed by the Secure64 Signer.

Vendor Response: None

Final Rating: Pass
### 7.5 Infobox: Scorecard Evaluation

<table>
<thead>
<tr>
<th>DNSSEC Signer Requirements</th>
<th>Weighted Value</th>
<th>Infoblox</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HA Support</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Gigabit Network Interfaces</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>IPv6 Support</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>NIST DNSSEC Best Practices</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Automatic Key Rollover</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Emergency Key Rollover</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Syslog Support</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Secure Remote Configuration Access</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>SNMP Monitoring</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Reversible Deployed Changes</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>DNS Server Software</td>
<td>Not Weighted</td>
<td>BIND</td>
</tr>
</tbody>
</table>

| **Security Features**                       |                |          |
| Internal Firewall                           | 9              |          |
| Keys can reside on logically separated network | 5              |          |
| Hardended OS                                | 9              |          |
| Update/Patchable                            | 9              |          |
| Keys Encrypted                              | 7              |          |
| Whole HDD Encrypted                         | 5              |          |
| Local Account Access                        | 9              |          |
| No Root Access                              | 5              |          |
| Knowledge of Vulnerabilities                | 9              |          |

| **Compatibility**                           |                |          |
| Compatible with existing infrastructure     | 9              |          |
| Non-DNSSEC enabled devices can read DNSSEC signed answers | 9              |          |

Total: 156 151

Figure 14: Infoblox Technical Scorecard (This illustration shows the technical evaluation of Infoblox.)
Figure 15: Infoblox Business Scorecard (This illustration shows the business evaluation of Infoblox.)

<table>
<thead>
<tr>
<th>DNSSEC Signer Requirements</th>
<th>Weighted Value</th>
<th>Infoblox</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value/Cost Feature</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Year Lifecycle/Support</td>
<td>Not Weighted</td>
<td>Yes</td>
</tr>
<tr>
<td>Warranty</td>
<td>Not Weighted</td>
<td>Yes</td>
</tr>
<tr>
<td>Vendor Installation Support</td>
<td>Not Weighted</td>
<td>Yes</td>
</tr>
<tr>
<td>Cost to implement</td>
<td>Not Weighted</td>
<td>TBD</td>
</tr>
<tr>
<td>Maintenance Cost</td>
<td>Not Weighted</td>
<td>TBD</td>
</tr>
<tr>
<td>Product Cost</td>
<td>Not Weighted</td>
<td>TBD</td>
</tr>
<tr>
<td>Product Lifecycle</td>
<td>Not Weighted</td>
<td>Yes</td>
</tr>
<tr>
<td>No Outside Purchase Required</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

7.6 Infoblox: Score Card Detailed Analysis

1. Hardware/Performance Features

**HA Support**

**Criterion Explanation:** This criterion denotes that the appliance is capable of syncing with one or more like appliances. If one of the appliances should malfunction, the services offered should be maintained with little or no disruption.

**Weighted Value:** 5

**Vendor Analysis:** The Infoblox appliance supports and high availability environment both through active/passive members and also through its Grid technology.

**Vendor Response:** An independent HA (high availability) pair provides hardware redundancy for the source of your network identity services. The two nodes that form an HA pair—identified as Node 1 and Node 2—are in an active/passive configuration. The active node receives, processes, and responds to all service requests. The passive node constantly keeps its database synchronized with that of the active node, so it can take over service if a failover occurs.

**Final Rating:** Pass

**Appendix References:** p. 173 - Infoblox Administration Guide.pdf
**Gigabit Network Interfaces**

**Criterion Explanation:** This criterion denotes that the appliance’s Ethernet ports support transmitting Ethernet frames at a rate of a gigabit per second, as defined by the IEEE 802.3-2008 standard.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance contains four Ethernet ports: Management, High Availability, LAN1 and LAN2. Each Ethernet port is capable of 10/100/1000 speeds.

**Vendor Response:** The MGMT port A 10/100/1000-Mbps Fast Ethernet port that you can use for device management or DNS service. You can enable the MGMT port and define its use through the GUI.

**Final Rating:** Pass

**Appendix References:** Appendix C: Figure 1, p. 5 - Infoblox User Guide for the Infoblox-1050, -1550, and -1552 Appliances.pdf

**IPv6**

**Criterion Explanation:** This criterion denotes that the appliance is capable of operating in an IPv6 addressing scheme.

**Weighted Value:** 1

**Vendor Analysis:** The Infoblox appliance’s networking stack support the routing of IPv6 addresses. The appliance also supports the management of IPv6 DNS records.

**Vendor Response:** You can use Grid Manager to manage IPv6 networks and their AAAA, PTR and host resource records. You can configure IPv6 networks and track IP address usage in those networks. You can also split and join IPv6 networks, when necessary. Note that the Infoblox appliance does not currently serve DHCP to IPv6 networks.

**Final Rating:** Pass

**Appendix References:** Appendix C: Figure 2, p. 683 - Infoblox Administration Guide.pdf

**NIST DNSSEC Best Practices**

**Criterion Explanation:** This criterion denotes that the appliance is capable of implementing all required NIST DNSSEC Best Practice Guidelines.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance implements all required NIST DNSSEC Best Practice Guidelines.
**Vendor Response:** The latest shipping version of Infoblox NIOS software has built-in support for DNSSEC and allows you to become compliant with the OMB mandate. Transparent to end users, DNSSEC by Infoblox can be configured with single clicks, and delivers automated, on-the-fly key generation and management using the latest technology and protocol features (BIND 9.6.1 with NSEC3 support). The result is faster adoption at a much lower cost requiring less in-house training and expertise.

**Final Rating:** Pass

**Appendix References:** p. 8 - wp_BPA_DNSSEC.pdf

---

**Automatic Key Rollover**

**Criterion Explanation:** This criterion denotes that the appliance is capable of exchanging expired key signing keys and zone signing keys with new pre-published keys.

**Weighted Value:** 1

**Vendor Analysis:** The Infoblox appliance supports automatic key rollover for the Zone Signing Key. The appliance supports notification of expire for both the Zone Signing Key and the Key Signing Key. The Key Signing Key must be manually rolled over.

**Vendor Response:** ZSK rollovers occur automatically on the grid master, using the double signature rollover method described in RFC 4641. This method provides for a grace period, which is half of the rollover period. The default ZSK rollover period is 30 days; thus the default grace period is 15 days. Unlike ZSK rollovers, which occur automatically, KSK rollovers must be initiated by an admin. When the KSK rollover is overdue or is due within seven days, the grid master displays a warning when administrators log in.

**Final Rating:** Pass

**Appendix References:** Appendix C: Figures 3 - 4, p. 533 - Infoblox Administrator Guide.pdf

---

**Emergency Key Rollover**

**Criterion Explanation:** This criterion denotes that the appliance permits administrators to manually exchange key signing keys and zone signing keys with new keys that have are not currently published.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance supports the functionality to unsign a zone in a case of a compromised Zone Signing Key or Key Signing Key.

**Vendor Response:** When you need to perform an emergency key rollover, you can unsign a zone and then re-sign it to generate new ZSK and KSK key pairs. When you unsign a zone, the grid master permanently removes all automatically generated DNSSEC records in the zone and parent zone.

**Final Rating:** Pass
Syslog Support

**Criterion Explanation:** This criterion denotes that the appliance is capable of exporting generated logs to a Syslog server.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance supports both local and remote comprehensive Syslog viewing.

**Vendor Response:** NIOS appliances generate syslog messages that you can view through the Syslog viewer and download to a directory on your management station. In addition, you can configure a NIOS appliance to send the messages to one or more external syslog servers for later analysis. Syslog messages provide information about appliance operations and processes. You can also include audit log messages and specific BIND messages among the messages the appliance sends to the syslog server.

**Final Rating:** Pass

**Appendix References:** Appendix C: Figure 6, p. 292 - Infoblox Administrator Guide.pdf

Secure Remote Configuration Access

**Criterion Explanation:** This criterion denotes that the appliance provides configuration access via either SSH or a web interface encrypted by an SSL or TLS connection.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance supports both HTTP of SSL and SSHv2.

**Vendor Response:** When you log in to the NIOS appliance, your computer makes an HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer protocol) connection to the NIOS appliance. HTTPS is the secure version of HTTP, the client-server protocol used to send and receive communications throughout the Web. HTTPS uses SSL (Secure Sockets Layer) to secure the connection between a client and server. SSL provides server authentication and encryption. The NIOS appliance supports SSL versions 2 and 3. SSH is at default disabled; SSHv2 can be enabled to allow superuser admins to access the Infoblox CLI from a remote location. This option can be set at both the grid and member levels.

**Final Rating:** True

**Appendix References:** Appendix C: Figures 7 - 10, pp. 36 & 216 - Infoblox Administrator Guide.pdf
Rack Mountable

**Criterion Explanation:** This criterion denotes that the appliance is equipped with proper hardware to be mounted in an equipment rack.

**Weighted Value:** 1

**Vendor Analysis:** The Infoblox appliance shipped with screws and is standardized to mount into an equipment rack.

**Vendor Response:** The appliance mounts into a standard 19” (48 cm) equipment rack.

**Final Rating:** Pass

**Appendix References:** Appendix C: Figure 11, p. 9 - Infoblox User Guide for the Infoblox-1050, -1550, and -1552 Appliances.pdf

SNMP Monitoring

**Criterion Explanation:** This criterion denotes that the appliance is capable of acting as a SNMP agent.

**Weighted Value:** 7

**Vendor Analysis:** The Infoblox appliance supports being queried for SNMP traps. SNMP can be configured both on the Grid and member level.

**Vendor Response:** You can configure a NIOS appliance as an SNMP-managed device so that an SNMP management station can send queries to the appliance and retrieve information from its MIBs.

**Final Rating:** Pass

**Appendix References:** Appendix C: Figure 12, p. 312 - Infoblox Administrator Guide.pdf

Revertible Deployed Changes

**Criterion Explanation:** This criterion denotes that the appliance permits administrators to revert running configurations to a previous configuration state.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance supports reverting individual configuration changes and also downgrading its running software.

**Vendor Response:** You can revert to a version of software that was previously running on your NIOS appliance. The NIOS appliance stores the previous software version in its backup software partition.

**Final Rating:** Pass
DNS Server Software

**Criterion Explanation:** This criterion describes the DNS server software running on the appliance.

**Weighted Value:** Not Weighted

**Vendor Analysis:** The Infoblox appliance operates off of a customized version of BIND.

**Vendor Response:** None

**Final Rating:** N/A

2. Security Features

**Internal Firewall**

**Criterion Explanation:** This criterion denotes that the appliance supports a self-regulating firewall.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance only had open ports for the services that were running, at the moment of testing.

**Vendor Response:** Ports on the Infoblox appliance are only opened with required for the current deployment architecture.

**Final Rating:** Pass

**Keys can reside on logically separated network**

**Criterion Explanation:** This criterion denotes that the appliance has the capability of storing its Key Signing Keys and Zone Signing Keys and that the appliance is not required to be publically facing.

**Weighted Value:** 5

**Vendor Analysis:** The DNSSEC keys are stored on the primary DNS server. This appliance does not have to be publically facing, in order for DNS to be operational, if a hidden master configuration is utilized.

**Vendor Response:** Using a hidden primary configuration allows you to run the primary name server for your external zones inside your firewall, where it will be better protected.

**Final Rating:** Pass
Appendix References: p. 5 - wp_BPA_DNSSEC.pdf

Hardened OS

Criterion Explanation: This criterion denotes that the appliance’s operating system has measures in place to reduce the likelihood of being compromised.

Weighted Value: 9

Vendor Analysis: None

Vendor Response: The appliance has been stripped of any unneeded services. The DNS daemon also operates in a jailed environment.

Final Rating: Conditional Pass

Update/Patchable

Criterion Explanation: This criterion denotes that the appliance is capable of updating its code base.

Weighted Value: 9

Vendor Analysis: The Infoblox appliance supports both incremental and full updates. Full updates may be tested before deployment. Downgrading to a previous software version is also supported.

Vendor Response: The appliance enables the administrator to upload new software to the grid manager, distribute the software upgrade files, optionally test the upgrade and perform the software upgrade.

Final Rating: Pass

Appendix References: p. 264 - Infoblox Administrator Guide.pdf

Keys Encrypted

Criterion Explanation: This criterion denotes that the appliance is capable of encrypting its Key Signing Keys and Zone Signing Keys via the means of software or hardware encryption.

Weighted Value: 7

Vendor Analysis: None

Vendor Response: The Infoblox appliance stores the Zone Singing Key and Key Singing Key in a distributed database, across one or more grid members, which is encrypted.

Final Rating: Conditional Pass
Whole HDD Encrypted

**Criterion Explanation:** This criterion denotes that the appliance is capable of fully encrypting its hard drive(s) with the exception of the master boot record.

**Weighted Value:** 5

**Vendor Analysis:** The Infoblox appliance does not support full disk encryption.

**Vendor Response:** None

**Final Rating:** Fail

Local Account Access

**Criterion Explanation:** This criterion denotes that the appliance allows local accounts and that granular permissions may be provisioned.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance supports the creation of local accounts. All account holders are considered administrators, but accounts can be defined with select access via group permissions.

**Vendor Response:** A user must have an admin account to log in to the NIOS appliance. Each admin account belongs to an admin group, which contains roles and permissions that determine the tasks a user can perform.

**Final Rating:** Pass

Appendix References: Appendix C: Figure 13, p. 71 - Infoblox Administrator Guide.pdf

No Root Access

**Criterion Explanation:** This criterion denotes that the appliance does not support the functionality of a root user account.

**Weighted Value:** 5

**Vendor Analysis:** There Infoblox appliance does not supply root access. Via both console and SSH, only an administrative Infoblox CLI is available for use.

**Vendor Response:** None

**Final Rating:** Pass
Knowledge of Vulnerabilities

**Criterion Explanation:** This criterion denotes that the appliance vendor has prior knowledge of security risks before they are announced to the public.

**Weighted Value:** 9

**Vendor Analysis:** None

**Vendor Response:** Infoblox works closely with both Internet Software Consortium (ISC) and US Computer Emergency Readiness Team (CERT) to gain knowledge of vulnerabilities before they are publically announced.

**Final Rating:** Pass

3. Compatibility

**Compatible with Existing Infrastructure**

**Criterion Explanation:** This criterion denotes that the appliance is capable of being installed as a DNSSEC signer in the University of Cincinnati’s planned DNS configuration.

**Weighted Value:** 9

**Vendor Analysis:** The Infoblox appliance is not meant to be used as a stand-alone DNSSEC signer, but as an appliance that provides DNS services with DNSSEC enabled. For the appliance to be implemented, the University’s current DNS architecture would be entirely replaced.

**Vendor Response:** None

**Final Rating:** Pass

**Non-DNSSEC enabled devices can read DNSSEC signed answers**

**Criterion Explanation:** This criterion denotes that non-DNSSEC enabled devices are capable of reading DNSSEC signed DNS responses that are signed by the appliance.

**Weighted Value:** 9

**Vendor Analysis:** A non-DNSSEC enabled client was able to read the DNS zone data that is signed by the Infoblox appliance.

**Vendor Response:** None

**Final Rating:** Pass
8. Recommendations

The analysis of the DNSSEC vendors was completed through the use of a weighted, unbiased grading criterion. The grading criterion was organized into two distinct divisions and then into subcategories, these divisions produced a technical scorecard and a business scorecard. A technical recommendation and a business recommendation have been developed from each scorecard. The technical recommendation for the University of Cincinnati DNSSEC Vendor Analysis is Infoblox with a final score of 142 points out of a possible total of 156 points. The business recommendation for the University of Cincinnati DNSSEC Vendor Analysis is a tie with BlueCat Networks and Infoblox; both have a final score of five points out of a possible total of five points. The business recommendation is limited to accurate quantifiable information; the University of Cincinnati must further weight tailored qualitative information, provided by each vendor. The final recommendation for the University of Cincinnati DNSSEC Vendor Analysis is Infoblox’s Network Services Appliance product.

9. Conclusion

The University of Cincinnati has requested an analysis of a solution to implement DNSSEC for the current DNS architecture. DNSSEC is a technology that provides security to the existing DNS protocol. DNSSEC, while still in its infancy of deployment, is a viable layer of security for the University to consider. This project has intended to provide the University with a solid understanding of DNSSEC, the current DNSSEC appliance market and a recommendation for the solutions which best meets the current requirements of the University of Cincinnati.
Appendix A: BlueCat Networks

Figure 1: HA Support (This illustration shows the configuration page for the BlueCat Networks Proteus’ XHA for High Availability.)

Figure 2: IPv6 (This illustration shows the configuration page for the BlueCat Networks Proteus’ IPAM for creating an IPv6 DNS block.)
Figure 3: IPv6 (This illustration shows the display page for the BlueCat Networks Proteus’ IPAM for IPv6 DNS blocks.)

Figure 4: Automatic Key Rollover (This illustration shows the configuration page for the BlueCat Networks Proteus’ DNSSEC signing policy to configure automatic ZSK key rollover.)
Figure 5: Emergency Key Rollover (This illustration shows the options page for the BlueCat Networks Proteus' DNSSEC ZSK emergency key rollover.)

Figure 6: Syslog Support (This illustration shows the configuration console for the BlueCat Networks Proteus to configure Syslog.)
"common-case", which means that, anyone can access the https, just that the traffic is encrypted. Please read the User Manual for details.

In Main Session mode, users can enable or disable the HTTPS support with the default settings or the configured settings. And also, users can show whether the HTTPS support is enabled.

```
> {enable | disable | show} https-support
When configuring/enabling/disabling HTTPS support, the HTTP support is not disabled by default, however, users can disable or enable HTTP support when HTTPS support is enabled.
> {enable | disable | show} http-support
```

In Configuration Mode, users can configure the https-support by setting expiry-days, organization-name, password, etc. To enter the configuration mode for configuring HTTPS support, type:

```
> configure https-support
To get the commands for configuring HTTPS-support, after entering the Configuration Mode, type "help".
For information on using the Configure Mode, type "help configure"
```

:Proteus:> enable https-support
Shutting down Proteus Server...

Figure 7: Secure Remote Configuration Access (This illustration shows the configuration console for the BlueCat Networks Proteus to enable SSL over HTTP.)
Figure 8: Secure Remote Configuration Access (This illustration shows the SSL self signed certificate issued by the BlueCat Networks Proteus when connecting to the Proteus via SSL over HTTP.)

Figure 9: Secure Remote Configuration Access (This illustration shows the RSA2 key fingerprint issued by the BlueCat Networks Proteus when connecting to the Proteus via SSH.)
Figure 10: Rack Mountable (This image shows the BlueCat Networks Proteus and Adonis and their ability to be rack mounted.)

Figure 11: SNMP Monitoring (This illustration shows the configuration page for the BlueCat Networks Proteus’ monitoring via SNMP.)
Figure 12: Revertible Deployed Changes (This illustration shows the options page for the BlueCat Networks Proteus’ data restore.)

Figure 13: Update/Patchable (This illustration shows the options page for the BlueCat Networks Proteus’ version management.)
Figure 14: Update/Patchable (This illustration shows the configuration page for the BlueCat Networks Proteus' software update.)

Figure 15: Update/Patchable (This illustration shows the configuration page for the BlueCat Networks Proteus to push patches to an Adonis.)
Appendix B: Secure64

Due to a Mutual Nondisclosure Agreement, manuals and screenshots are not permitted within the dissertation. Manuals and screenshots can be requested for internal use of University of Cincinnati only.
Appendix C: Infoblox

Figure 1: HA Support (This illustration shows the configuration page for high availability for the Infoblox appliance.)

Figure 2: IPv6 (This illustration shows the configuration page for local network settings, which allows IPv6, for the Infoblox appliance.)
Figure 3: Automatic Key Rollover (This illustration shows the configuration page for DNSSEC which includes settings for KSK and ZSK rollover intervals, for the Infoblox appliance.)

Figure 4: Manual Key Rollover (This illustration shows the options page for the Infoblox appliance’ DNSSEC KSK manual key rollover.)
Figure 5: Manual Key Rollover (This illustration shows the options page for the Infoblox appliance' DNSSEC ZSK emergency key rollover.)

Figure 6: Syslog Support (This illustration shows the configuration page for the Infoblox appliance' Syslog.)
Figure 7: Secure Remote Configuration Access (This illustration shows the SSL self signed certificate issued by the Infoblox appliance when connecting to the appliance via SSL over HTTP.)

Figure 8: Secure Remote Configuration Access (This illustration shows the options page for issuing an SSL certificate by the Infoblox appliance.)
Figure 9: Secure Remote Configuration Access (This illustration shows the RSA2 key fingerprint issued by the Infoblox appliance when connecting to the appliance via SSH.)

Figure 10: Secure Remote Configuration Access (This illustration shows the options page to enable or disable SSH access.)
Figure 11: Rack Mountable (This image shows the Infoblox appliance and its ability to be rack mounted.)

Figure 12: SNMP Monitoring (This illustration shows the configuration page for the Infoblox appliance’ monitoring via SNMP.)
Figure 13: Update/Patchable (This illustration shows the configuration page for the Infoblox appliance' software update.)

Figure 13: Local Account Access (This illustration shows the configuration page for the Infoblox appliance.)
## Appendix D: Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BIND</strong></td>
<td>BIND (Berkeley Internet Name Domain) is an implementation of the DNS protocol. The BIND DNS server is used on the vast majority of Internet nameservers, and is the reference implementation of the DNS specification.</td>
</tr>
<tr>
<td><strong>Chain of Trust</strong></td>
<td>This term describes how a validating resolver finds a path from keys that it is configured to trust to your zone. Normally a resolver starts from the root and works its way to your zone.</td>
</tr>
<tr>
<td><strong>Cryptocard</strong></td>
<td>A cryptographic card (coprocessor) considerably speeds up the encoding and signature of cryptographic transactions while at the same time providing highly secure storage that is tamper proof and secure key handling.</td>
</tr>
<tr>
<td><strong>dig</strong></td>
<td>The <code>dig</code> command is used to query DNS servers; it is more flexible than the deprecated <code>nslookup</code> command.</td>
</tr>
<tr>
<td><strong>DMZ</strong></td>
<td>A Demilitarized Zone (DMZ) is a network segment that is separated from other networks. Many organizations will use a DMZ to separate their Local Area Networks (LANs) from the Internet to put additional security between their corporate network and the public Internet. Common items to be placed in a DMZ are public facing servers. For example, if an organization maintains their website on a server, that web server could be placed in the DMZ. This way if the machine would ever be compromised, the remainder of the company's network is not in danger.</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>DNS (the Domain Name System) provides mapping of hostnames to IP addresses and back again.</td>
</tr>
<tr>
<td><strong>DNSKEY</strong></td>
<td>A DNSSEC record type used to store a public key.</td>
</tr>
<tr>
<td><strong>DNSSEC</strong></td>
<td>Extensions to the DNS service that provide mechanisms for signing and securely resolving DNS data.</td>
</tr>
<tr>
<td><strong>DS</strong></td>
<td>A DNSSEC record type used to secure a delegation.</td>
</tr>
<tr>
<td><strong>EDNS</strong></td>
<td>Enhanced Domain Naming System (EDNS). An alternative root server system outside Internet governance that administers top level domain names not already in use.</td>
</tr>
<tr>
<td><strong>EDUCAUSE</strong></td>
<td>EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.</td>
</tr>
<tr>
<td><strong>HA</strong></td>
<td>High Availability (HA) refers to the availability of resources in a computer system, in the wake of component failures in the system.</td>
</tr>
<tr>
<td><strong>IANA</strong></td>
<td>The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources.</td>
</tr>
<tr>
<td><strong>ICANN</strong></td>
<td>Oversee a number of Internet-related tasks previously performed directly on behalf of the U.S. government by other organizations, notably the Internet Assigned Numbers Authority (IANA).</td>
</tr>
<tr>
<td><strong>Islands of Trust</strong></td>
<td>A signed zone that does not have an authentication chain from its delegating parent zone.</td>
</tr>
<tr>
<td><strong>ITAR</strong></td>
<td>The Interim Trust Anchor Repository, or ITAR, acts as a mechanism to disseminate “trust anchors” that have been provided by the operators of top-level domains who use DNSSEC to secure their zones. IANA is responsible for managing the DNS root zone, and uses these existing trust relationships to</td>
</tr>
</tbody>
</table>
verify the supplied trust anchors come from the correct party.

<table>
<thead>
<tr>
<th><strong>Key Signing Key (KSK)</strong></th>
<th>The KSK is an authentication key that corresponds to a private key used to sign one or more other signing keys for a given zone.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nameserver</strong></td>
<td>A nameserver is a server which has been set up to answer DNS queries, and provides information about a certain set of domains.</td>
</tr>
<tr>
<td><strong>NIST</strong></td>
<td>The National Institute of Standards and Technology (NIST) is a federal technology agency that develops and promotes measurement, standards, and technology.</td>
</tr>
<tr>
<td><strong>NSD</strong></td>
<td>Name Server Daemon (NSD) is an authoritative only, high performance, simple and open source name server.</td>
</tr>
<tr>
<td><strong>NSEC</strong></td>
<td>A DNSSEC record type used to prove non-existence of a DNS name.</td>
</tr>
<tr>
<td><strong>NSEC3</strong></td>
<td>The third version of NSEC which has higher security. See NSEC.</td>
</tr>
<tr>
<td><strong>RFC</strong></td>
<td>The Internet Engineering Task Force (IETF) codifies the decisions it comes to in documents called &quot;Requests For Comments&quot;. These are almost universally called by their acronym &quot;RFCs&quot;. Many RFCs are the standards on which the Internet is formed.</td>
</tr>
<tr>
<td><strong>Root Server</strong></td>
<td>The root servers are nameservers that all other nameservers on the Internet know about, and contain very basic information about the DNS system, which will lead other servers along the path to finding out specific information about a host.</td>
</tr>
<tr>
<td><strong>RRSIG</strong></td>
<td>A DNSSEC record type used to hold a signature which covers a set of DNS records for a particular name and type.</td>
</tr>
<tr>
<td><strong>RSASHA1</strong></td>
<td>This algorithm specifies a key-type of RSA in which signatures are generated using the SHA-1 signature algorithm. Keys can be of many lengths, depending on their intended use. Zone-signing keys are often 1024 bits or larger, and key-signing keys are often 2048 bits or larger.</td>
</tr>
<tr>
<td><strong>SHA-1</strong></td>
<td>A 160-bit digest algorithm. This is a mandatory algorithm for DS and DLV records, and most of the key algorithms use it when signing. SHA-1 is designed by the National Security Agency of USA and published as their government standard.</td>
</tr>
<tr>
<td><strong>Signed Zone</strong></td>
<td>A zone whose records are signed as defined by RFC 4035 [7] Section 2. A signed zone contains DNSKEY, NSEC, RRSIG, and DS records. These records allow DNS data to be validated by resolvers.</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td>Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks.</td>
</tr>
<tr>
<td><strong>SOA</strong></td>
<td>This is a record which every zone must have exactly one of. It describes some general characteristics about the zone, such as who to contact about it, which nameservers to send dynamic updates to, important serial numbers, and timing parameters.</td>
</tr>
<tr>
<td><strong>SSL</strong></td>
<td>Secure Socket Layer (SSL) is a session layer protocol that provides authentication and confidentiality to applications.</td>
</tr>
<tr>
<td><strong>TLS</strong></td>
<td>Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet.</td>
</tr>
<tr>
<td><strong>Trust Anchor</strong></td>
<td>A trust anchor specifies the key stores that contain trusted root certificates.</td>
</tr>
<tr>
<td><strong>TSIG</strong></td>
<td>Transaction Signature (TSIG) is a computer networking protocol used by the Domain Name System (DNS) as a way to authenticate updates to a dynamic DNS database. The RFC 2845 specification specifically states that the TSIG</td>
</tr>
</tbody>
</table>
The protocol allows for transaction level authentication using shared secrets and one way hashing.

**Zone Signing Key (ZSK)**

An authentication key that corresponds to a private key used to sign a zone.

### Appendix E: Bibliography


