PCI Compliance Considerations and Barracuda Load Balancer Deployment

https://campus.barracuda.com/doc/12194992/

This article refers to firmware 4.2.1 and higher. You can install the latest firmware from the **ADVANCED > Firmware Updates** page in the Barracuda Load Balancer web interface.

This article outlines implementation considerations when deploying the Barracuda Load Balancer in an environment subject to PCI Data Security Standard (PCI DSS) compliance. This article focuses on the requirements placed on the Barracuda Load Balancer for achieving PCI compliance, in an environment that includes the following:

- Barracuda Load Balancer
- Application Server
- Database Server

For **PCI DSS Requirement 6.6 compliance** and added application security, consider including a Barracuda Web Application Firewall in your deployment environment.

Efficient PCI Compliance

PCI Compliance applies to entities that process, store, or transmit cardholder data. The Barracuda Load Balancer intelligently distributes traffic among servers for efficient use of server resources, and provides server fail-over for High Availability. The Barracuda Load Balancer, as an underlying technology infrastructure in your network, does not directly manage or store cardholder data. However, it provides a secure environment for the transmission of all application data including cardholder data. For merchants subject to PCI DSS, this facilitates certification attainment.

According to section 4.1 of the ***Payment Card Industry (PCI) Data Security Standard v1.2***, merchants handling credit card data are required to **"...use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks."**

Deploying services behind the Barracuda Load Balancer simplifies your PCI compliance by relying on a secure, up-to-date PCI-compliant stack front-end for back-end servers. Additionally, the Barracuda Load Balancer provides risk mitigation and business continuity by relieving your certification process from full scanning, and operating system, middle-ware, and application update and patching on all your Internet-facing production servers which can result in downtime and administrator overhead.

An information supplement to the PCI DSS notes that as long as the servers behind a load balancer are configured similarly, they are exempt from an internal scan. For more information, refer to ***Account for Load Balancers*** *(page 14 of the* ***PCI Approved Scanning Vendors Program Guide****)*.

Configure Front End SSL

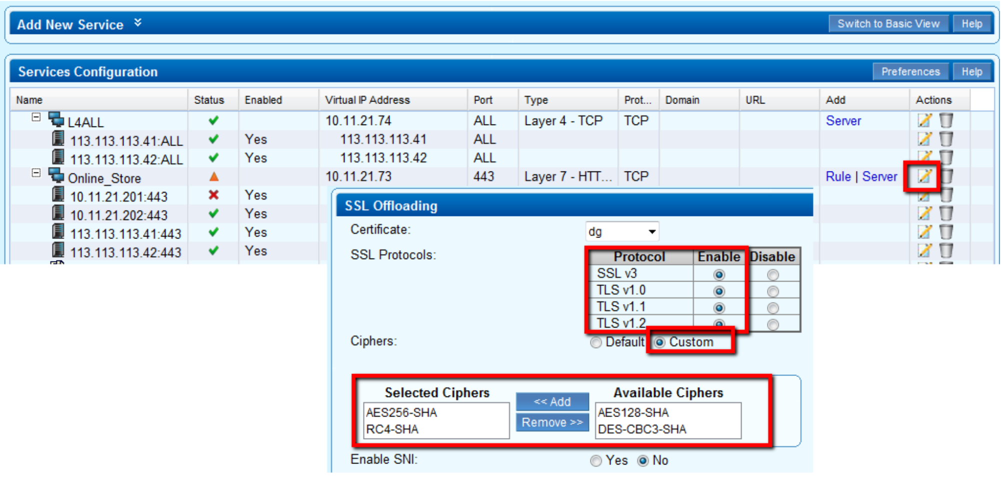
Front-end SSL refers to the SSL implemented between the Barracuda Load Balancer and the client connecting to the Barracuda Load Balancer from the Internet. Configure SSL for each Service that requires compliance.

The use of SSL has the following security implications under PCI DSS compliance:

1. Disables Secure Sockets Layer version 2 (SSLv2);
2. Disallows "weak" cryptography;
3. Quarterly PCI security vulnerability scans conducted against your external-facing PCI systems.

Without the first two measures, the scans are likely to fail, leading to falling out of compliance and the associated risks and consequences.

Barracuda Load Balancer provides secure SSL Offloading for your services. To enable this, log into the Barracuda Load Balancer web interface, go to the **BASIC > Services** page, and click **Edit** following the Service you wish to modify. In the edit screen, scroll to the **SSL Offloading** section:



Services Configuration

Name	Status	Enabled	Virtual IP Address	Port	Type	Prot...	Domain	URL	Add	Actions
L4ALL	✓		10.11.21.74	ALL	Layer 4 - TCP	TCP			Server	
113.113.113.41:ALL	✓	Yes	113.113.113.41	ALL						
113.113.113.42:ALL	✓	Yes	113.113.113.42	ALL						
Online_Store	▲		10.11.21.73	443	Layer 7 - HTT...	TCP			Rule | Server	
10.11.21.201:443	✗	Yes								
10.11.21.202:443	✓	Yes								
113.113.113.41:443	✓	Yes								
113.113.113.42:443	✓	Yes								

SSL Offloading

Certificate: dg

SSL Protocols:

Protocol	Enable	Disable
SSL v3	●	○
TLS v1.0	●	○
TLS v1.1	●	○
TLS v1.2	●	○

Ciphers: ○ Default ● Custom

Selected Ciphers	Available Ciphers
AES256-SHA RC4-SHA	AES128-SHA DES-CBC3-SHA

Enable SNI: ○ Yes ● No

By default the Barracuda Load Balancer disables the deprecated ciphers and protocols, and is therefore "secure by default". As shown in the screenshot above, the Barracuda Load Balancer enables only:

- Secure Protocols – SSL v3, TLS v1.0/1.1/1.2
- Secure Ciphers – all weak and medium ciphers are disabled

Additionally, security researchers have recently identified new vulnerabilities in the SSL protocol; these are mitigated by the secure SSL stack in the Barracuda Load Balancer as shown in *Table 1.*

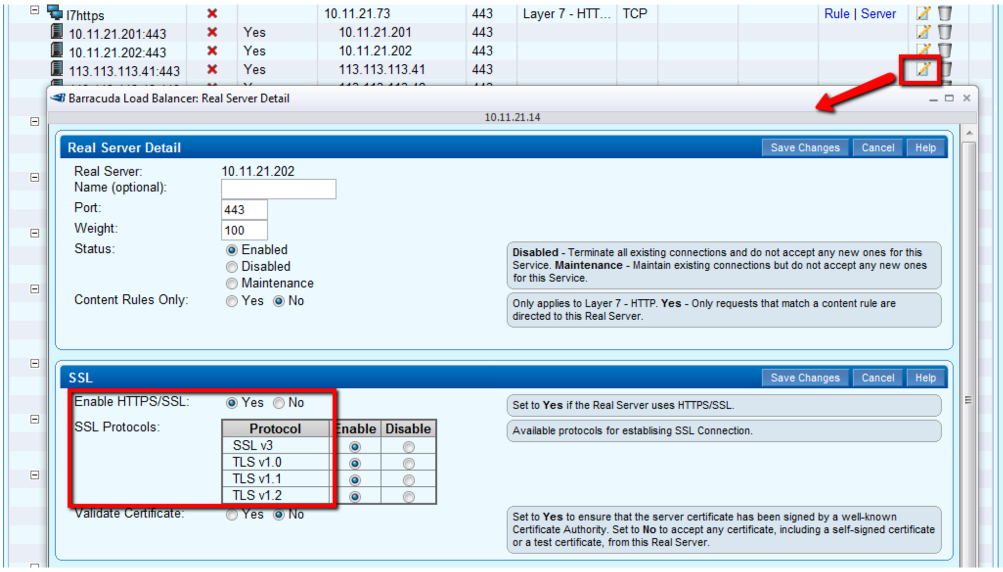
Table 1. SSL Protocol Vulnerabilities

Vulnerability	Impact	Remediation
Insecure Renegotiation	High	Barracuda Load Balancer only supports secure renegotiation initiated by the Server.
BEAST Attack	Low	SSL v3 and TLS 1.0 may be vulnerable to this attack even when block ciphers are used; configure the Barracuda Load Balancer to prioritize or enforce stream (RC4) cipher suites.
CRIME Attack	Low	This attack exploits the protocol compression feature. By default, SSL compression is disabled in the Barracuda Load Balancer.

Configuring Back-End SSL

Back-end SSL refers to the use of the SSL protocol to re-encrypt traffic between the Barracuda Load Balancer and the back-end servers. PCI mandates SSL when transmitting data over "open, public" networks; see ***Requirement 4: Encrypt transmission of cardholder data across open, public networks*** *(page 35 of the* ***PCI Data Security Standard****).* When the path between the Barracuda Load Balancer and the servers is within a secure zone, organizations are not mandated to re-encrypt the traffic assuming the “privacy” of the path can be demonstrated for compliance.

If your network architecture, environment, or the associated risk necessitates back-end SSL, go to the **BASIC > Services** page, click **Edit** following the Service you wish to modify, and update the **SSL** section as shown in the following image:



l7https	✖		10.11.21.73	443	Layer 7 - HTT...	TCP	Rule | Server
10.11.21.201:443	✖	Yes	10.11.21.201	443			
10.11.21.202:443	✖	Yes	10.11.21.202	443			
113.113.113.41:443	✖	Yes	113.113.113.41	443			

Barracuda Load Balancer: Real Server Detail

10.11.21.14

Real Server Detail

Real Server: 10.11.21.202

Name (optional):

Port: 443

Weight: 100

Status: ● Enabled ○ Disabled ○ Maintenance

Disabled - Terminate all existing connections and do not accept any new ones for this Service. **Maintenance** - Maintain existing connections but do not accept any new ones for this Service.

Content Rules Only: ○ Yes ● No

Only applies to Layer 7 - HTTP. **Yes** - Only requests that match a content rule are directed to this Real Server.

SSL

Enable HTTPS/SSL: ● Yes ○ No

Set to **Yes** if the Real Server uses HTTPS/SSL.

SSL Protocols:

Protocol	Enable	Disable
SSL v3	●	○
TLS v1.0	●	○
TLS v1.1	●	○
TLS v1.2	●	○

Available protocols for establising SSL Connection.

Validate Certificate: ○ Yes ● No

Set to **Yes** to ensure that the server certificate has been signed by a well-known Certificate Authority. Set to **No** to accept any certificate, including a self-signed certificate or a test certificate, from this Real Server.

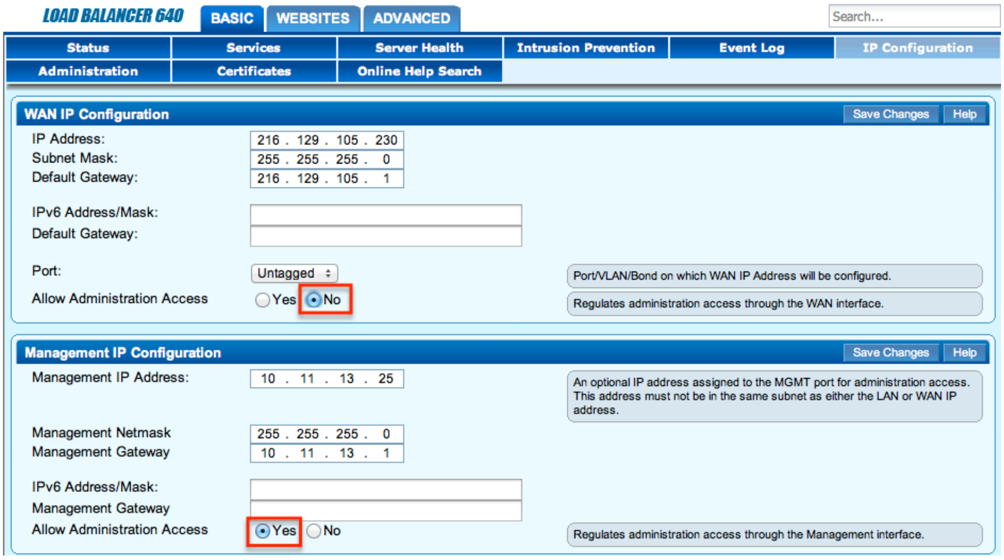
Back-end SSL uses the same secure SSL protocols and ciphers as front-end SSL.

Secure Certificates

Though PCI does not specify minimum certificate key sizes, Barracuda Network recommends a minimum of 2048 bit key strength when renewing certificates or deploying new services. Note that the National Institute for Standards and Technology (NIST) has mandated moving to 2048 bit certificates, which the Barracuda Load Balancer fully supports. Ensure that all SSL services, as well as the Management UI, employ strong certificates.

Secure the Web-based Management UI

Barracuda Networks recommends allowing the Management UI access only from the Management interface and disabling it from the WAN interface. This ensures that the Management UI is not exposed to external scanners and access is restricted to an internal, secure management network. To configure this, go to the **BASIC > IP Configuration** page, and update the **WAN IP Configuration** section as shown in the following image:



WAN IP Configuration

IP Address: 216 . 129 . 105 . 230
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway: 216 . 129 . 105 . 1

IPv6 Address/Mask:
Default Gateway:

Port: Untagged — Port/VLAN/Bond on which WAN IP Address will be configured.
Allow Administration Access ○ Yes ● No — Regulates administration access through the WAN interface.

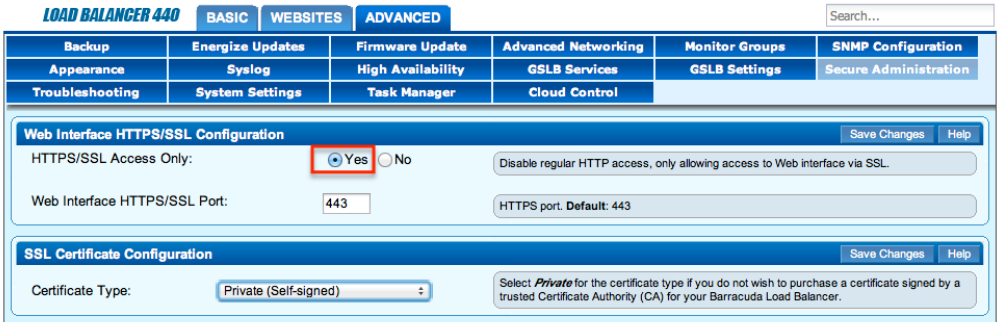
Management IP Configuration

Management IP Address: 10 . 11 . 13 . 25 — An optional IP address assigned to the MGMT port for administration access. This address must not be in the same subnet as either the LAN or WAN IP address.

Management Netmask 255 . 255 . 255 . 0
Management Gateway 10 . 11 . 13 . 1

IPv6 Address/Mask:
Management Gateway
Allow Administration Access ● Yes ○ No — Regulates administration access through the Management interface.

For additional security, restrict Web Interface access by setting **HTTPS/SSL Access Only** to *Yes*, and disable regular HTTP access on the **ADVANCED > Secure Administration** page. You can select a Private certificate if you have restricted access to a private network as in the screenshot shown above. If you choose to enable access via the WAN interface, ensure that you select a Trusted certificate instead.



Web Interface HTTPS/SSL Configuration

HTTPS/SSL Access Only: ● Yes ○ No — Disable regular HTTP access, only allowing access to Web interface via SSL.

Web Interface HTTPS/SSL Port: 443 — HTTPS port. **Default**: 443

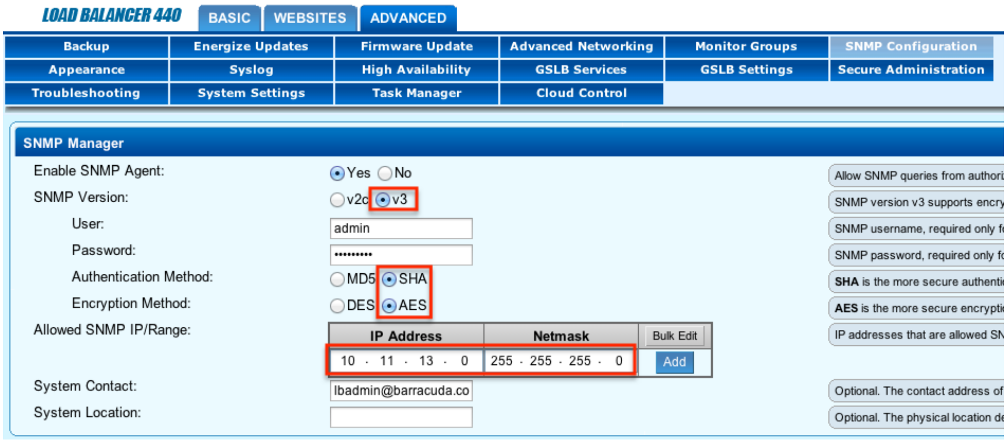
SSL Certificate Configuration

Certificate Type: Private (Self-signed) — Select *Private* for the certificate type if you do not wish to purchase a certificate signed by a trusted Certificate Authority (CA) for your Barracuda Load Balancer.

Secure SNMP Access

To secure the SNMP access for compliance, go to the **ADVANCED > SNMP Configuration** page, and complete the following steps:

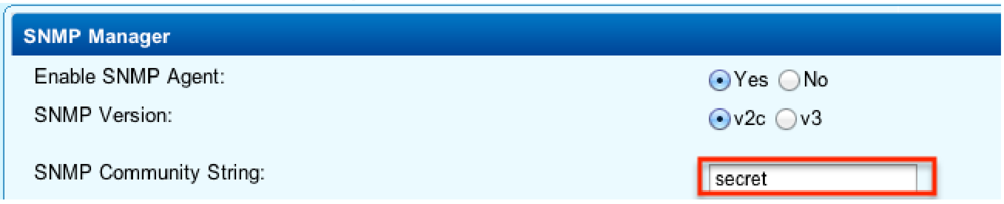
1. In the **SNMP Manager** section, select the **SNMP Version** as **v3**.
2. Provide a secure password for the admin user.
3. Select **SHA** and **AES** as the **Authentication Method** and **Encryption Method** respectively; these are more secure than MD5 and DES.
4. Restrict SNMP Access to an internal network via the **Allowed SNMP IP/Range** control:



SNMP Manager

Enable SNMP Agent:	● Yes ○ No	Allow SNMP queries from authori
SNMP Version:	○ v2c ● v3	SNMP version v3 supports encry
User:	admin	SNMP username, required only f
Password:	••••••••	SNMP password, required only fo
Authentication Method:	○ MD5 ● SHA	**SHA** is the more secure authenti
Encryption Method:	○ DES ● AES	**AES** is the more secure encrypti
Allowed SNMP IP/Range:	IP Address: 10 . 11 . 13 . 0 Netmask: 255 . 255 . 255 . 0	IP addresses that are allowed SN
System Contact:	lbadmin@barracuda.co	Optional. The contact address of
System Location:		Optional. The physical location de

5. If you choose to use SNMP v2c to support legacy SNMP clients, ensure that you change the default **SNMP Community String**:


SNMP Manager

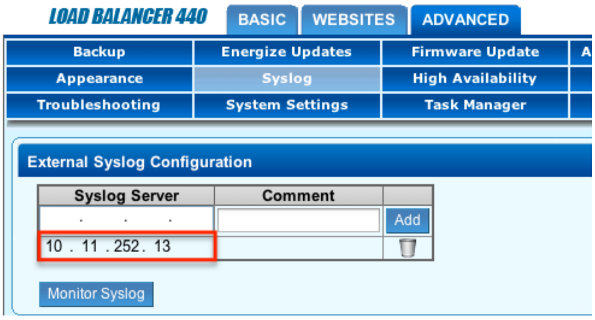
Enable SNMP Agent:	● Yes ○ No
SNMP Version:	● v2c ○ v3
SNMP Community String:	secret

For details on scanner false positives with respect to SNMP, refer to PCI-DSS Requirement 4 later in this article.

Enable Syslog for Audit Compliance

Continuous activity log monitoring alerts you to any unusual activity on the Barracuda Load Balancer.

To enable Syslog, go to the **ADVANCED > Syslog** page, enter the Syslog Server address, and click **Add**:



External Syslog Configuration

Syslog Server	Comment
. . .	
10 . 11 . 252 . 13	

Ensure Password Security

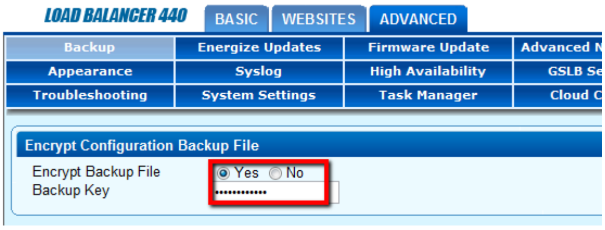
Before you install and deploy one or more Barracuda Load Balancers, ensure that you have changed the default password on all devices. It is recommended that you have an organizational policy in place for setting passwords with a minimum strength that are distinct from personal passwords used by employees on the public Internet.

Enabling HTTPS/SSL only access to the web-based interface, as noted earlier in this article, further enhances credential security over public and private networks.

> The console and web-based interface use separate passwords; be sure to change both passwords.

Encrypt All Configuration Backups

Ensure that all manual and automated backups are encrypted so that configuration and sensitive information is not compromised in the event the backup file is compromised. To configure encryption on all configuration backups, go to the **ADVANCED > Backup** page, and set **Encrypt Backup File** to *Yes.*



Encrypt Configuration Backup File

Encrypt Backup File ● Yes ○ No

Backup Key ••••••••••••

Specify a strong **Backup Key** using the same principals used for strong passwords. This key is required to decrypt or restore the backup configuration.

Additional PCI Compliance

Barracuda Networks is committed to security of its devices and helping customers achieve compliance. Barracuda Networks has additional best-of-breed security product offerings that can help you achieve additional PCI compliance cost effectively, especially for web application security, email encryption, anti-virus, and web filtering.

Customers evaluating Barracuda Networks products can be assured of security and compliance commitment throughout the product’s life cycles. For any issues or questions related to PCI compliance, contact Barracuda Networks Technical Support or your sales representative.

Scanner False Positives

Following are two false positives that some scanners have reported during PCI evaluations.

SNMP vulnerability

Some scanners incorrectly report that the Barracuda Load Balancer is susceptible to CVE 2002-0012 CVE 2002-0013 CVE2002-0053.

Barracuda Load Balancer includes a customized port of NET-SNMP version: 5.4.2.1, which is not susceptible to the vulnerabilities mentioned in the reports. Only versions of NET-SNMP prior to 4.2.2 are susceptible to these.

For additional information refer to **CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)** available at **http://www.cert.org/advisories/CA-2002-03.html**.

If you encounter this false positive, submit the report to the scanning organization for validation.

Additionally, Barracuda Networks has implemented the following additional security measures as recommended by the security advisory:

- Ability to filter SNMP traffic from non-authorized internal hosts
- Ability to change default community strings
- Ability to disable SNMP service if not explicitly required

Insecure Cookies

The Barracuda Load Balancer inserts cookies for a service when the Persistence type is HTTP Cookies. Some scanners confuse these with application cookies and report them as insecure if the HTTP only or secure attribute is not set. You can configure both of these from the Persistence properties of a Service to avoid this false positive.

Figures

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.