PCI Compliance Considerations

https://campus.barracuda.com/doc/19333214/

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

- Barracuda Load Balancer ADC
- Application Server
- Database Server

For PCI DSS Requirement 6.6 compliance and added application security, consider purchasing an Application Security license for the Barracuda Load Balancer ADC.

Efficient PCI Compliance

PCI Compliance applies to entities that process, store, or transmit cardholder data. The Barracuda Load Balancer ADC intelligently distributes traffic among servers for efficient use of server resources, and provides server fail-over for High Availability. The Barracuda Load Balancer ADC, 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 ADC 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 ADC 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 ADC are configured similarly, they are exempt from an internal scan. For more information, refer to *Account for Load Balancer ADCs (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 ADC and the client connecting to the Barracuda Load Balancer ADC 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 ADC provides secure SSL Offloading for your services. To enable this, log into the Barracuda Load Balancer ADC web interface, go to the **BASIC > Services** page, select a service, and scroll down to the **SSL Settings** section:

SSL Settings

SSL — On / Off

SSL Protocols
- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

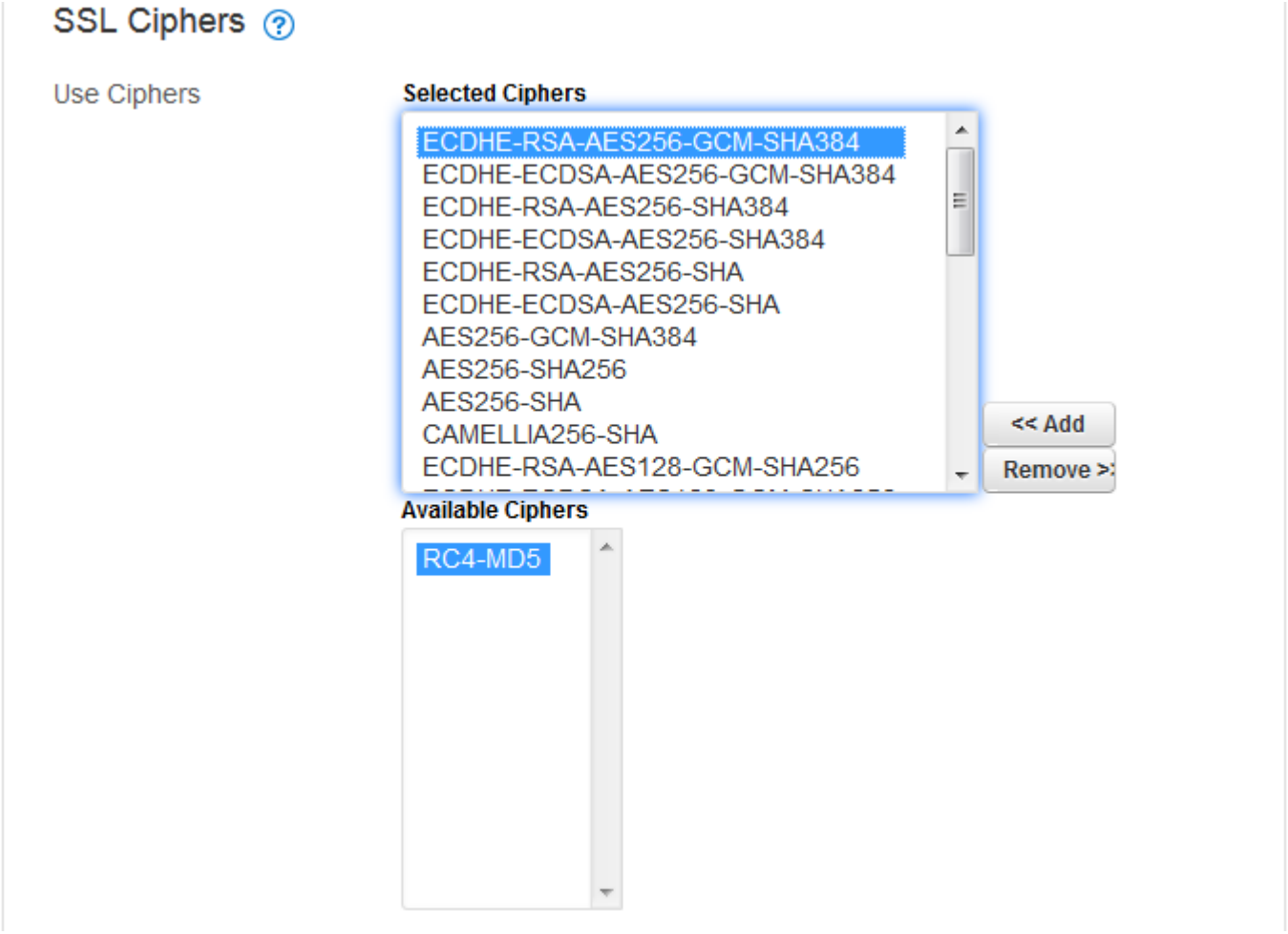
Advanced Options — Hide

Enable Perfect Forward Secrecy — Yes / No
Enable DH key exchange with ephemeral keys. This ensures the keys used for each connection are newly generated and provides Perfect Forward Secrecy.

Client Authentication — Enable / Disable
*When set to **Enable**, users connecting to this Service must present their certificate which is validated using a Trusted certificate. Trusted certificates are uploaded on the **BASIC > Certificates** page in the **Upload Trusted (CA) Certificate** section.*

Enforce Client Certificate — Yes / No
*Set to **Yes** if you want clients to present their certificate while connecting to the service. If the clients fail to present their certificate, the SSL handshake is immediately terminated.*

Trusted Certificates
*Select one or more trusted certificates for validating the certificates presented by the clients connecting to this Service. Only those client certificates that are signed by one of these trusted certificates are allowed access. Upload trusted certificates on the **BASIC > Certificates** page.*



By default the Barracuda Load Balancer ADC disables the deprecated cipher and is therefore "secure by default". As shown in the screenshots above, the Barracuda Load Balancer ADC enables only:

- SSL Protocols – SSL v3, TLS v1.0/1.1/1.2
- SSL Ciphers – Only the RC4-MD5 cipher is disabled. All other ciphers are enabled (see **Selected Ciphers**).

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 ADC as shown in *Table 1.*

Table 1. SSL Protocol Vulnerabilities

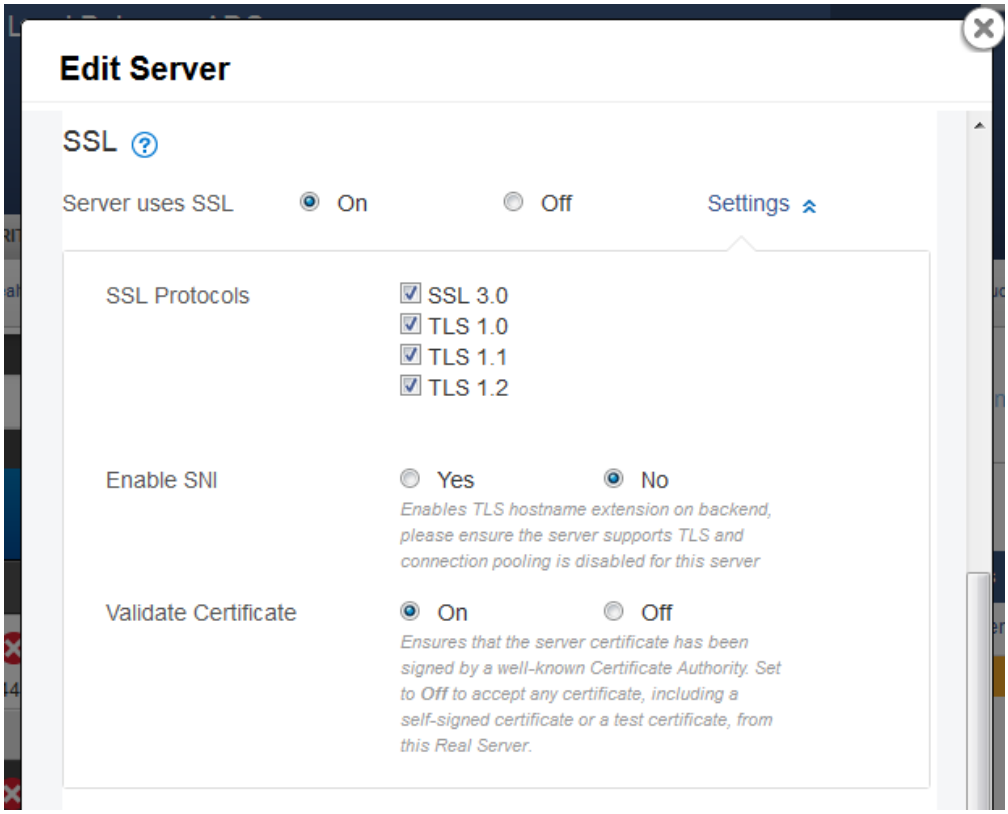
Vulnerability	Impact	Remediation
Insecure Renegotiation	High	Barracuda Load Balancer ADC only supports secure renegotiation initiated by the Server.
BEAST Attack	Low	SSL v3 and TLS 1.0 may be vulnerable to this attack even when block ciphers are used; configure the Barracuda Load Balancer ADC to prioritize 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 ADC.

Configuring Back-End SSL

Back-end SSL refers to the use of the SSL protocol to re-encrypt traffic between the Barracuda Load Balancer ADC 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 ADC 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** for the Server you wish to modify, and update the **SSL** section as shown in the following image:



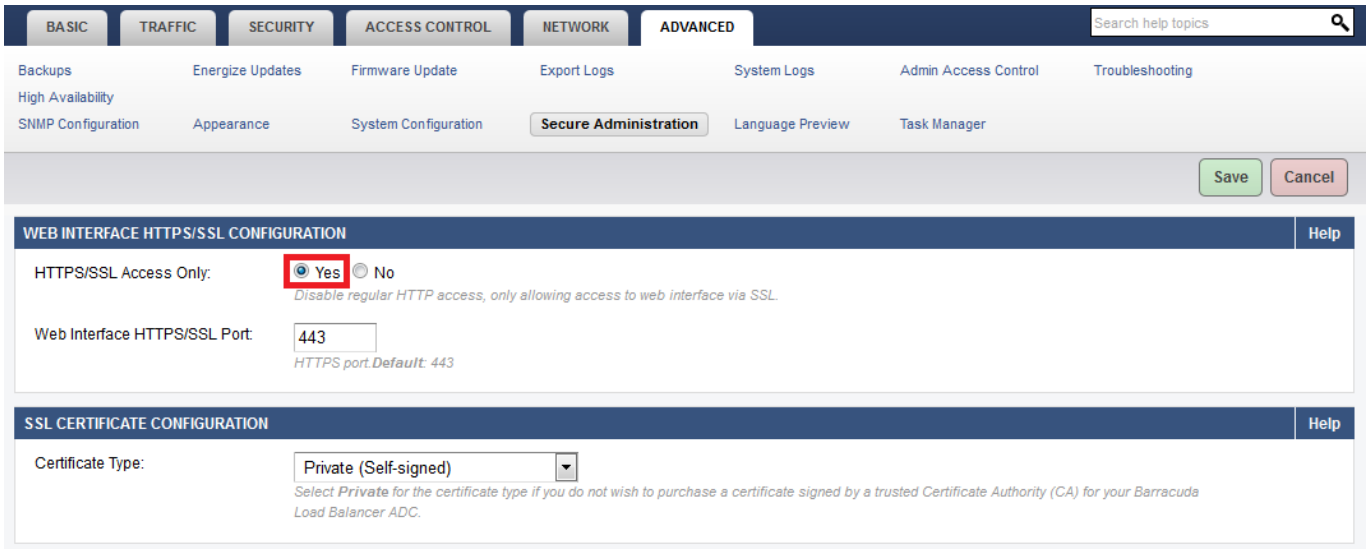
Back-end SSL uses the same secure SSL protocols and ciphers as front-end SSL.

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 ADC fully supports. Ensure that all SSL services, as well as the Management UI, employ strong certificates.

Secure the Web-based Management UI

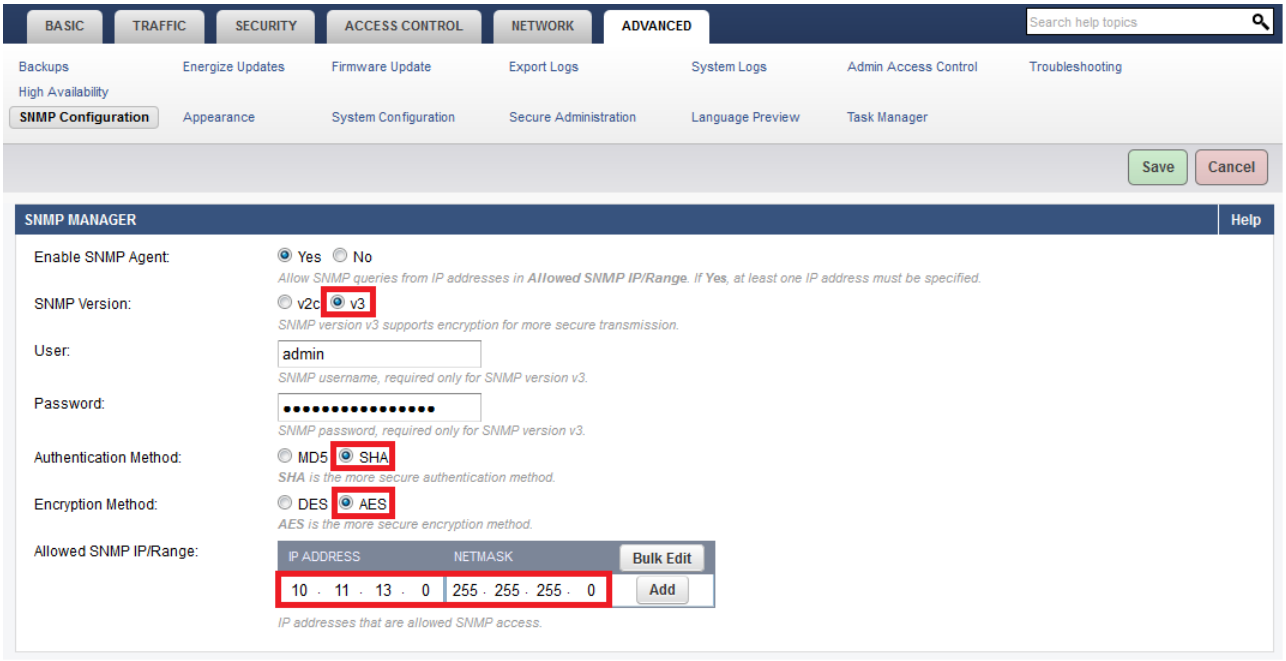
To allow Web Interface access by HTTPS/SSL only, enable HTTPS/SSL Access Only to Yes on the **ADVANCED > Secure Administration** page. You can select a Private certificate if you have restricted access to a private network as in the screenshot shown above.



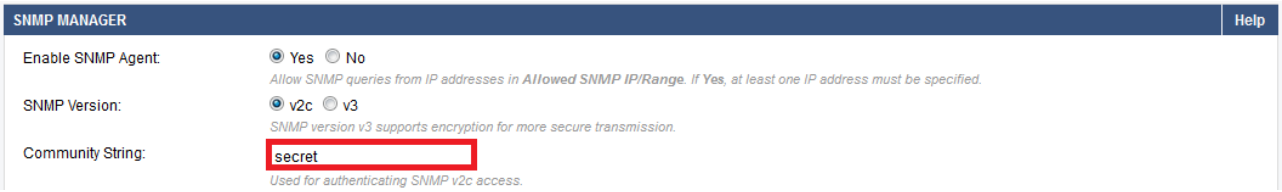
Secure SNMP Access

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:



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



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

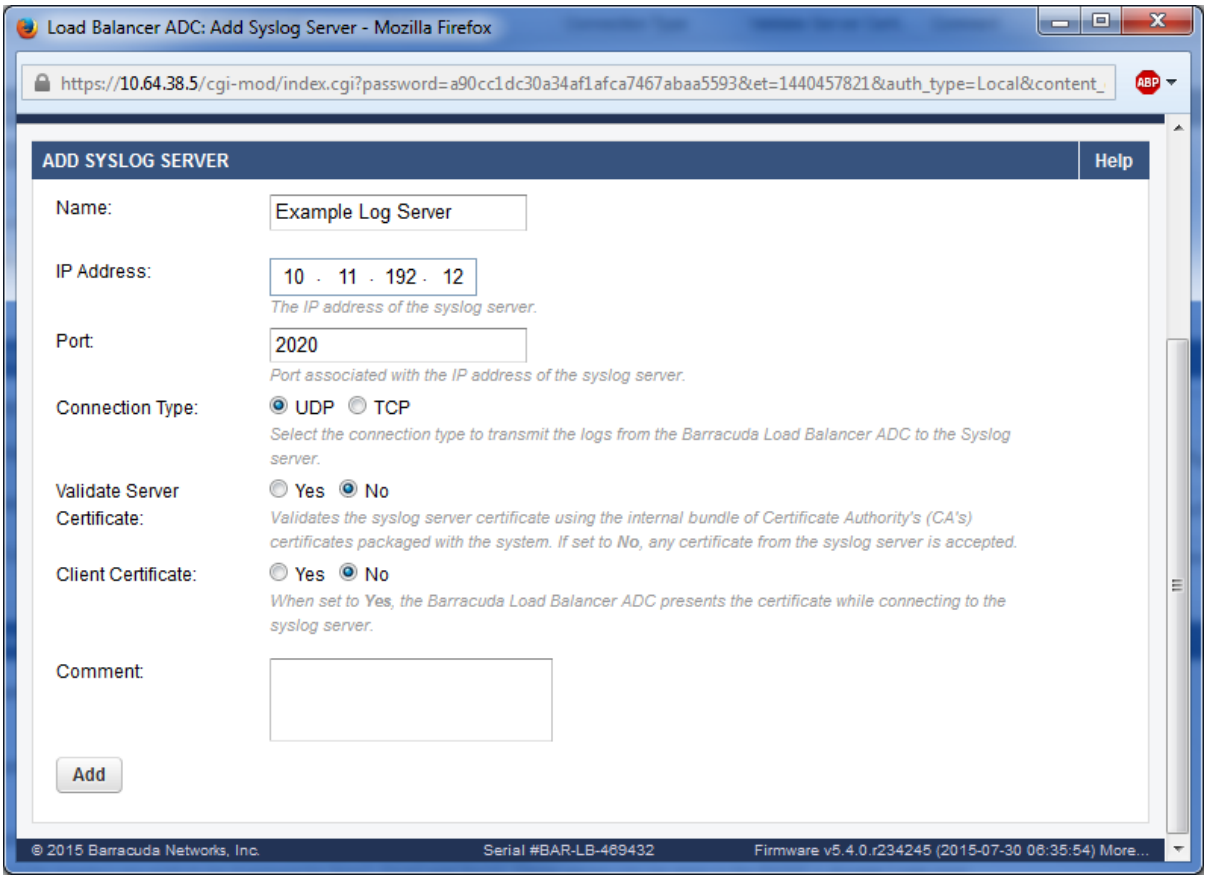
Continuous activity log monitoring alerts you to any unusual activity on the Barracuda Load Balancer ADC.

To enable Syslog:

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Syslog** section, click **Add Syslog Server**. The **Add Syslog Server** window appears.
3. Specify values for the following fields:
    1. **Name** – Enter a name to identify this syslog server.

2. **IP Address** - Enter the IP address of the syslog server.
3. **Port** – Enter the port associated with the IP address of the syslog server.
4. **Connection Type** – Select the connection type to transmit the logs from the Barracuda Load Balancer ADC to the Syslog server.
5. **Validate Server Certificate** – Set to *Yes* to validate the syslog server certificate using the internal bundle of Certificate Authority's (CAs) certificates packaged with the system. If set to **No**, any certificate from the syslog server is accepted.
6. **Client Certificate** – When set to *Yes*, the Barracuda Load Balancer ADC presents the certificate while connecting to the syslog server.

4. Click Add.



Ensure Password Security

Before you install and deploy one or more Barracuda Load Balancer ADCs, 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.

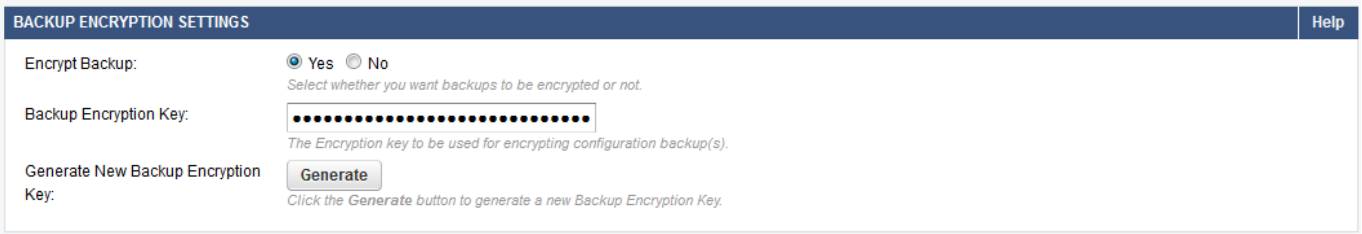
Enabling HTTPS/SSL-only access to the web-based interface, as noted earlier in this article, further

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 > Backups** page, and set **Encrypt Backup** to **Yes**.



Click **Generate** to create a strong encryption key for your backup file. A new window opens with the generated key. Copy this key into the **Backup Encryption Key** field. This key is required to decrypt or restore the backup configuration. Click **Save** when you have finished.

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 ADC is susceptible to CVE 2002-0012 CVE 2002-0013 CVE2002-0053.

Barracuda Load Balancer ADC 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) (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 ADC inserts cookies for a service when the Persistence type is set to 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