

PCI Compliance Considerations and Barracuda Load Balancer Deployment

https://campus.barracuda.com/doc/4108/

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 <u>Barracuda Web Application Firewall</u> 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 <u>Account for Load Balancers</u> (page 14 of the <u>PCI Approved Scanning Vendors</u> <u>Program Guide</u>).

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:

Add New Service 🛛 🎽									Switch to Bas	sic View H
Services Configuration									Pref	erences
Name	Status	Enabled	Virtual IP Address	Port	Туре	Prot	Domain	URL	Add	Actions
😑 🖶 L4ALL	 Image: A second s		10.11.21.74	ALL	Layer 4 - TCP	TCP			Server	20
📕 113.113.113.41:Al	.L 💙	Yes	113.113.113.41	ALL						20
📕 113.113.113.42:Al	.L 💙	Yes	113.113.113.42	ALL						2.0
Online_Store	A		10.11.21.73	443	Layer 7 - HTT	TCP			Rule Server	1 🛛 🖉
10.11.21.201:443	×	Yes	CCL Officializa							
10.11.21.202:443	 Image: A second s	Yes	SSL Officialing				-			2 🗍
113.113.113.41:44	3 💙	Yes	Certificate:		dg	•				2 🔟
113.113.113.42:44	3 💙	Yes	SSL Protocols:			Protoco	ol Enabl	e Disable		2
			Ciphers:			L v3 S v1.0 S v1.1 S v1.2 efault	Custom			
			Selected C AES256-SHA RC4-SHA	Ciphers	Add Remove >> DE	Availal S128-SH S-CBC3	ole Ciphers HA B-SHA			

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:



17.0	~		10 11 21 72	442	Lavor 7 HTT	TCD	Dula L Saniar	2 17
1/https	÷ .	00	10.11.21.75	443	Layer / - HTT	TCP	Rule Server	
	÷ .	es loc	10.11.21.201	443				
	Ŷ,	65	113 113 113 41	443				
113.113.113.41.443		,	140 140 140 10	440				
Barracuda Load Balance	r: Real Serve	er Detail						
C				10.1	1.21.14			
Real Server Detail							Save Changes Cancel	Help
Real Server:	10.11	.21.202						
Name (optional):								
Port:	443							
Weight:	100							
Status:	E E E	nabled			Disabled - Terminate	e all existing connect	tions and do not accept any new ones for	this
	D	isabled			Service. Maintenand	ce - Maintain existin	g connections but do not accept any new	ones
Orabert Dates Oaks	() M	laintenance			Tor tilla Service.			
Content Rules Only:	© Y	es 💿 No			Only applies to Layer directed to this Real S	7 - HTTP. Yes - On Server	ly requests that match a content rule are	
								=
SSL							Save Changes Cancel	Help
Enable HTTPS/SSL:	@ Y	es 💿 No			Set to Yes if the Real	Server uses HTTPS	S/SSL.	
SSL Protocols:		Protocol	Enable Disable		Available protocols for	or establising SSL C	onnection.	
	SS	L v3	0 0					
	TLS	S v1.0	0 0					
	TLS	3 v1.1	0 0					
Woldow Continue	115	5 v1.2						
validate Certificate:	ΘY	es 💿 No			Set to Yes to ensure Certificate Authority.	that the server cert Set to No to accept	ificate has been signed by a well-known any certificate, including a self-signed cer	tificate

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:



LOAD BALANCER 640	BASIC WEBSIT	TES ADVANCED			Search
Status	Services	Server Health	Intrusion Prevention	Event Log	IP Configuratio
Administration	Certificates	Online Help Search			
AN IP Configuration					Save Changes He
P Address:	216 . 129 .	105 . 230			
Subnet Mask:	255 . 255 .	255.0			
Default Gateway:	216 . 129 .	. 105 . 1			
Pv6 Address/Mask					
Default Cateway:					
Derault Gateway.					
Port:	Untagged	•	Port/VLAN/Bond on with	nich WAN IP Address will	be configured.
Allow Administration Acc	ess OYes OI	No	Regulates administrati	on access through the W	AN interface.
anagement IP Configu	ration				Save Changes H
Vanagement IP Address	10 . 11 .	. 13 . 25	An optional IP address This address must not address.	assigned to the MGMT t be in the same subnet a	oort for administration access s either the LAN or WAN IP
Vanagement Netmask	255 . 255 .	. 255 . 0			
Management Gateway	10 . 11 .	. 13 . 1			
Pv6 Address/Mask:					
Management Gateway					
Allow Administration Acc					

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.

LOAD BALANCER 44	BASIC WEBSIT	ES ADVANCED			Search
Backup	Energize Updates	Firmware Update	Advanced Networking	Monitor Groups	SNMP Configuration
Appearance	Syslog	High Availability	GSLB Services	GSLB Settings	Secure Administration
Troubleshooting	System Settings	Task Manager	Cloud Control		
Web Interface HTTPS// HTTPS/SSL Access C Web Interface HTTPS/	SSL Configuration Duly:	• Yes No	Disable regular HTTP access, c	inly allowing access to Web in	Save Changes Help Interface via SSL.
SSL Certificate Config	uration				Save Changes Help
Certificate Type:	Private (Self-signe	d) 🗘	Select <i>Private</i> for the certificate trusted Certificate Authority (CA	type if you do not wish to pur) for your Barracuda Load Ba	chase a certificate signed by a lancer.

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:



LOAD BALANCER 4	40 BASIC WEBSIT	ES ADVANCED			
Backup	Energize Updates	Firmware Update	Advanced Networking	g Monitor Groups	SNMP Configuration
Appearance	Syslog	High Availability	GSLB Services	GSLB Settings	Secure Administration
Troubleshooting	System Settings	Task Manager	Cloud Control		
SNMP Manager					
Enable SNMP Agent:		⊙Yes ⊝No			Allow SNMP queries from aut
SNMP Version:		⊙v2c⊙v3			SNMP version v3 supports er
User:		admin			SNMP username, required or
Password:		•••••			SNMP password, required or
Authentication	Method:	MD5 OSHA			SHA is the more secure auth
Encryption Met	hod:	OES OAES			AES is the more secure encry
Allowed SNMP IP/Ra	nge:	IP Address	Netmask	Bulk Edit	IP addresses that are allowed
		10 · 11 · 13 · 0	255 · 255 · 255 · 0	Add	
System Contact:		lbadmin@barracuda.co			Optional. The contact addres
System Location:					Optional. The physical location

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
SNMP Community String:	secret

For details on scanner false positives with respect to SNMP, refer to <u>PCI-DSS Requirement 4</u> 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**:

LOAD BALANCER 44	BASIC WEBSITE	S ADVANCED	
Backup	Energize Updates	Firmware Update	A
Appearance	Syslog	High Availability	
Troubleshooting	System Settings	Task Manager	
External Syslog Config	guration Comment		
		Add	
10 11 252 12			
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 <u>HTTPS/SSL only access</u> 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.*

LOAD BALANGER 44	BASIC WEBSITE	S ADVANCED	
Backup	Energize Updates	Firmware Update	Advanced N
Appearance	Syslog	High Availability	GSLB Se
Troubleshooting	System Settings	Task Manager	Cloud C
Encrypt Configuration	Backup File		

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 <u>Barracuda Networks Technical Support</u> 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 <u>CERT[®] Advisory CA-2002-03 Multiple Vulnerabilities in Many</u> <u>Implementations of the Simple Network Management Protocol (SNMP)</u> available at <u>http://www.cert.org/advisories/CA-2002-03.html</u>.

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.

Barracuda Load Balancer



Figures

- 1. service_config01.png
- 2. pci_compliance.png
- 3. config_ui.png
- 4. securing.png
- 5. snmp.png
- 6. secret.png
- 7. syslog.png
- 8. encryption.png

© Barracuda Networks Inc., 2025 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.