WHITE PAPER

PCI DSS 2.0 COMPLIANCE

WITH AETHRA TELECOMMUNICATIONS ROUTERS AND INTEGRATED ACCESS DEVICES.

Issue 1 - May 9 2017

A TLC srl / Copyright © 2016-2020 All Rights Reserved / Legal Office: Via Pierfranco Bonetti, 88/90 – 00128 Roma - Italy
Operating Office: Via 1° Maggio, 26 - Ancona - Italy / Phone: +39 071 250 651 / Email: info@aethra.com / VAT: IT10652521005

INTRODUCTION

Aethra Telecommunications Routers and Integrated Access Devices include high-end security features that can be used to help businesses ensure that all the payment data and transaction are protected according to the specifications of the Payment Card Industry (PCI) Data Security Standard.

Business stores that need to achieve PCI DSS Compliance can secure the access portion of their network using the Aethra Telecommunications Routers and Integrated Access Devices.

1. PCI DSS 2.0 REQUIREMENTS

The following tables show which features of the Aethra Telecommunications Routers and Integrated Access Devices need to be used to help achieve the compliancy to the specific requirement.

GOALS	PCI DSS REQUIREMENTS
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Table 1 – PCI DSS Requirements.

Aethra Telecommunications Routers and Integrated Access Devices are routers with integrated firewall, VPN and ACLs and can be configured to segment the network to ensure the compliance to PCI DSS:

- advanced routing features and VRF-Lite are used to direct the traffic between different networks and isolate different zones, preventing sensitive information to be carried in non-secure areas;
- Access Control Lists (ACLs) can be used to restrict traffic between the cardholder data environment

A TLC srl / Copyright © 2016-2020 All Rights Reserved / Legal Office: Via G.B. Martini, 2 - 00198 Roma - Italy
Operating Office: Via 1° Maggio, 26 - Ancona - Italy / Phone: +39 071 250 651 / Email: info@aethra.com / VAT: IT10652521005

and the rest of the network;

- Stateful Firewall can be used to restrict traffic between the cardholder data environment and the rest of the network;
- VPN can be used to encrypt traffic;
- TACACS / TACACS+ can be used to restrict access to cardholder data and to track all the management accesses and the configuration changes on the router;
- Aethra Telecommunications routers and Integrated Access Devices can be configured to use an AAA model for user-based access.

REQUIREMENT	AETHRA TELECOMMUNICATIONS ROUTER AND IAD FEATURE
Install and maintain a firewall configuration to protect data.	Stateful firewall
Do not use vendor-supplied defaults for system passwords and other security parameters.	Aethra Telecommunications Operating System
Protect stored cardholder data	N/A
Encrypt transmission of cardholder data and sensitive information across public networks	IPSec VPN / GRE
Use and regularly update antivirus software	N/A
Develop and maintain secure systems and applications	Aethra Telecommunications is sensible to check and track all the potential security vulnerabilities; software upgrades are released with comprehensive list of enhancements and bugfixes
Restrict access to data by business need	AAA / TACACS
Assign a unique ID to each person with computer access	TACACS client can be used to support this requirement
Restrict physical access to cardholder data	N/A
Track and monitor all access to network resources and cardholder data	N/A
Regularly test security systems and processes	N/A
Maintain a policy that addresses information security for employees and contractors	N/A

Table 2 – PCI DSS Requirements Mapping to Aethra Telecommunications Features.

A TLC srl / Copyright © 2016-2020 All Rights Reserved / Legal Office: Via G.B. Martini, 2 - 00198 Roma - Italy
Operating Office: Via 1° Maggio, 26 - Ancona - Italy / Phone: +39 071 250 651 / Email: info@aethra.com / VAT: IT10652521005

Copyright© A TLC srl 2016-2020 – All rights reserved

Disclaimer

The information provided in this document is subject to change without notice, and should not be construed as a commitment or as an implied warranty of merchantability.

A TLC srl / Copyright © 2016-2020 All Rights Reserved / Legal Office: Via G.B. Martini, 2 - 00198 Roma - Italy
Operating Office: Via 1° Maggio, 26 - Ancona - Italy / Phone: +39 071 250 651 / Email: info@aethra.com / VAT: IT10652521005