The PCI Standard

How Nile supports PCI requirements for LAN and WLAN

PCI Compliance
www.nilesecure.com

Table of Contents

Background

What is the PCI Security Standard?

The PCI Security Standards Council's mission is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

The PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to develop and drive the adoption of data security standards and resources for safe payments worldwide.

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you accept or process payment cards, PCI DSS applies to you.

How does Nile support your PCI requirements?

Our technology supports your security parameters.

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.

Any access to the cardholder environment or transmission of cardholder data does not go through the Nile cloud. Nile's Cloud services are out of scope for your PCI Audit.

The Nile Service Block (NSB) is fully owned and managed by Nile. Nile elements (AP's, Sensors, Headend, and Switches) cannot be linked to any other switches or devices. Nile NSB security ensures that only Nile elements can communicate with each other in a zero-trust model - meaning all elements must authenticate each other before communicating.

Nile has obtained ISO27001 and SOC2 Type 2 for our data centers. Additionally, Nile has completed PCI DSS 3.0 self-assessment questionnaire.

Firewall based network segmentation

PCI DSS Requirement # 1

1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

PCI requires that Cardholder Data Environment (CDE) access needs to be restricted by appropriate network segmentation. The Nile Service fully supports network segmentation.

With Nile, it's possible to use the same WLAN and protect the traffic to the CDE using a firewall. Nile supports integration with industry-leading firewall providers.

With the inherent support of segmentation, Nile also has the capability to isolate IoT devices from CDE traffic.

Wireless Environment

PCI DSS Requirement # 2

2.1.1	For wireless environments connected to the CDE or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

Nile's NSB does not contain any default keys and Nile elements work based on a zero-trust model and provides the highest level of security using certificates. Nile NSBs do not use SNMP.

Wireless Data Transmission and Authentication

PCI DSS Requirement # 3

4.1.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:

Nile supports various forms of secure authentication in SSID Modes. Following list has various levels of secure authentication that customers can choose from.

1. *WPA2 Personal*
2. *WPA2 Enterprise*
3. *WPA3 Personal (strict)*
4. *WPA3 Personal (transition)*
5. *WPA3 Enterprise 192-bit (strict)*
6. *WPA3 Enterprise (strict)*
7. *WPA3 Enterprise (transition)*
8. *Captive Portal (with SSO Federation support)*

Patching

PCI DSS Requirement # 4

6	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release
6.5.3	Insecure cryptographic storage
6.5.4	Insecure communications

Nile Service Blocks (NSBs) are always automatically updated to the latest version directly from the Nile Cloud. Nile can push security patches and updates in real-time to all the devices within the Nile Service Block. Nile portal and Nile Guest service are continuously tested for vulnerabilities and patched in real-time.

Access Control

PCI DSS Requirement # 5

7.1.1	System components and data resources that each role needs to access for their job function. Level of privilege required (for example, user, administrator, etc.) for accessing resources.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibility

Nile has separated privileged access by providing Root, Administrator, and Monitor user only roles within the Nile portal.

Strong Cryptography

PCI DSS Requirement # 6

8.2.1a	Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage.

NSB uses the Trusted Platform Module (TPM) to protect cryptographic data in devices and MACsec for wired data transmission.

Physical Access

PCI DSS Requirement # 7

9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

All devices within the NSB environment are tamper-proof. Nile does not have any open console or USB port.

Logging and Monitoring

PCI DSS Requirement # 8

10.3	Record at least the following audit trail entries for all system components for each event.
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

Nile provides ways to store the audit and event logs into desired SIEMS platforms (like Splunk) facilitating in a centralized location of logs. This is in addition to logs and events retention that Nile provides.

Protect Wireless Access Points

PCI DSS Requirement # 9

11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.
12.9.5	Include alerts from intrusion detection, intrusion-prevention, and file integrity monitoring systems.

Nile wireless IDS/IPS service scans the wireless spectrum to detect any presence of unauthorized, rogue access points, security attack tools, and interferers which can impact the Nile service, and sends alerts to customers.

Conclusion

Network security is a major priority for organizations and businesses, globally. 52% of organizations say that network security is a top concern when it comes to managing their network[5]. Traditional networks are made up of multiple wired and wireless components including layered on security elements which can be complex to maintain.

The Nile network eliminates the challenge of layering multiple components to building a secure enterprise network and the complexities that come with it. Nile's unique ability to design a holistic architecture enabled a new network-as-a-service model that is designed with security as a foundational element. It's built in every facet of the Nile architecture for zero-trust access, for a secure network, and for secure cloud. Zero-trust capabilities authenticates every user to ensure your network, data, and applications are protected against unauthorized access. Users are grouped based on their access privileges, traffic is encrypted from end-to-end, and user metadata is always protected. Included with your Nile service is management and upkeep of the network. Now, your IT teams do not have be burdened with refreshing hardware or pushing out security patches – it's on Nile. Nile automatically performs your hardware lifecycle refreshes, software upgrades and security patches to ensure your network is fine-tuned for optimal performance.

Security is a number one priority for you and for us.

5 IDC: Network as a Service Enables Flexible Consumption of Secure and Agile Enterprise Networks

Appendix

Nile Service Block (NSB)	The Nile Service Block is made up of natively built access points, switches, Head End, and sensors. Its unique tamper-resistant design physically secures the network– no device can directly plug into the network without being authenticated first.
MACsec	MACsec is an IEEE standard for security in wired ethernet LANs. It secures all traffic within a LAN environment. MACsec based LAN connection to the CDE environment is highly secure and reliable.