Technical Report

Security in the Cloud: The NetApp Private Storage for Cloud Solution

Guidelines for Understanding the NetApp Private Storage for Cloud Solution

Product Security Team, NetApp

November 2017 | TR-4648

Abstract

This guide describes the NetApp® Private Storage for Cloud (NPS) solution. The NPS solution encompasses many elements in order to provide a unified and secure storage infrastructure that enables an organization to bring traditional data centers and new architectures into the unified fabric. The solution enables the business to move, store, and manage data across flash, disk, and cloud resources in a unified manner. The guidance and solutions provided in this document are designed to help organizations understand the NPS solution.

TABLE OF CONTENTS

LIST OF FIGURES

1 Introduction

The evolution of today's landscape continues to present organizations with unique challenges in protecting their most valuable assets (data and information). The advanced and dynamic threats and vulnerabilities of today are ever increasing in sophistication. A key architecture that addresses the dynamics of today's ever-changing and fast-paced environment while securing vital resources and information is the NPS solution. The NPS solution is a cloud-connected solution that enables an organization to quickly and securely deploy a storage solution with industry-leading cloud vendors while maintaining complete control over an organization's data on a dedicated NetApp storage system.

NPS consists of the following use cases (including those that extend the functionality and capabilities of an organization):

- Software as a service (SaaS)
- Infrastructure as a service (IaaS)
- Big data analytics
- Regulatory and compliance requirements
- Ability to expedite agility and storage needs with rapid scale-out capabilities
- Ability to maintain control of data at all times
- Ability to maintain low latency for database applications
- Ability to provide high-throughput direct connections to the cloud
- Centralized storage intelligence through NetApp OnCommand® Insight
- Migration flexibility for cloud applications

For more information regarding NPS use cases, see the NetApp Verified Architecture for NetApp Private Storage for Cloud.

1.1 NPS Shared Responsibility Model

You have data that you are planning to host in the cloud. How does that affect security? What are the implications? What do you need to know? The key to understanding cloud security is understanding that it is based on a shared responsibility model. The shared responsibility model establishes that, regardless of cloud provider, the customer is responsible for security "in" the cloud, while the provider is responsible for security "of" the cloud. In other words, the customer is responsible for maintaining the security posture of their data whether it be in the cloud or on the premises. The cloud should be an extension of the organization and therefore should invoke the same security controls.

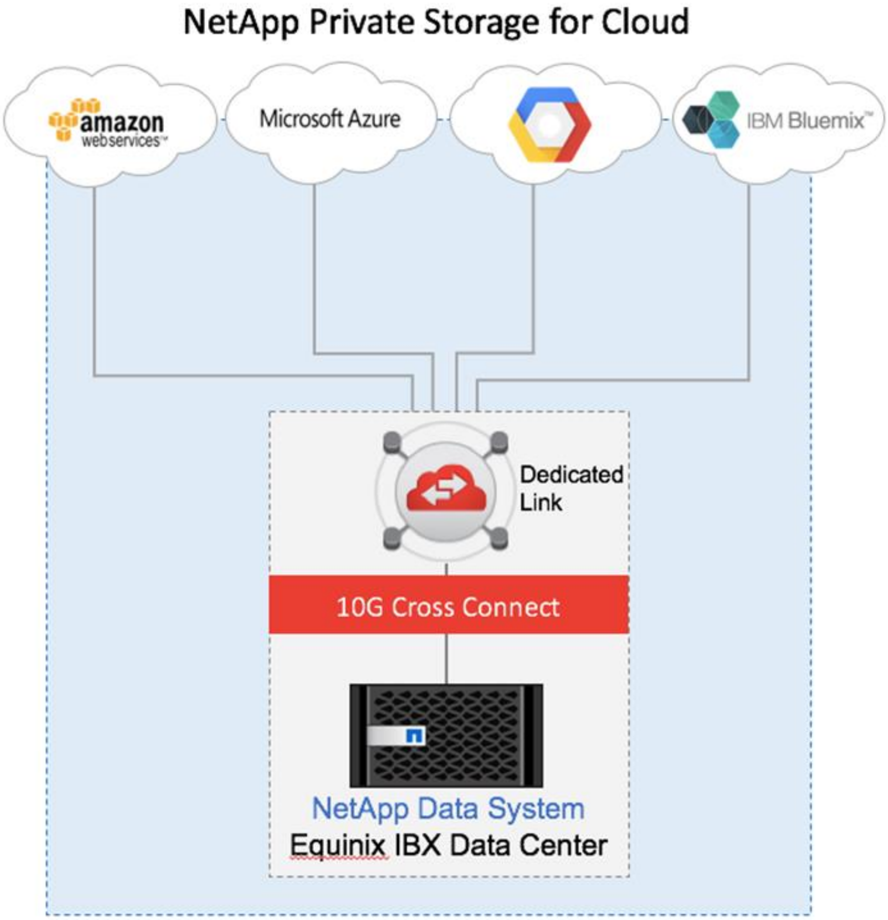
It is important to understand that while the shared responsibility models for each cloud provider might in fact be different, the responsibility for an organization's data always remains the responsibility of the organization.

This topic is covered in more detail in the Addressing Data Security section of this document.

2 NPS Architecture

Understanding the NPS solution begins with understanding the NPS architecture. The NPS solution leverages a NetApp storage system (FAS, FlexArray®, or all-flash storage), which is located in a colocation facility (data center). The colocation facility is most often Equinix; however, the NPS solution allows for flexibility, and other colocation facilities are also permitted. As depicted in Figure 1, the colocation facility provides a direct and dedicated high-bandwidth, low-latency network connection to a vendor public cloud such as Amazon Web Services (AWS), Microsoft Azure, or IBM Bluemix. This connection enables the use of IaaS and SaaS offerings for an organization.

Figure 1) NPS standard architecture.



The standard NPS architecture combines the computing resources of the cloud (either AWS, Azure, or Bluemix) to be deployed in a colocation data center facility and connected to NetApp hardware or software-based storage solutions. In addition, the colocation facility incorporates a switch and/or router for connectivity and encryption needs. The following additional protocols and configurations are also incorporated if needed:

- Routing protocols
- Virtual routing and forwarding (VRF) for segmentation
- VPN/security services
- Cloud or direct exchange
- Additional customer-provided network/connectivity equipment

For further details and infographics regarding the NPS solution, see the NPS for Cloud Infographic.

2.1 Cloud Support

Another key element of NPS is the cloud support, which provides flexibility and agility for the NPS solution. Leveraging NPS as a service allows organizations to leverage cloud providers for compute and additional resources, while maintaining security of the data through the use of protected colocation facilities. In addition, the NPS as a service solution allows organizations to take advantage of hyperscaler technology through compute, virtual routing, and advanced network capabilities.

For more details regarding NPS as a service, visit the NetApp Private Storage as a Service portal.

3 Addressing Data Security

In addition to understanding the NPS solution, today's organizations are also faced with making sure that all architectures are secured and extend the posture of their current environmental needs, including the following:

- **Governance, risk, and compliance (GRC).** Organizations must address guidelines and regulations such as the Federal Risk and Authorization Management Program (FedRAMP) and the General Data Protection Regulation (GDPR). The NPS solution addresses key elements such as segmentation and isolation through the colocation architecture for secure access, virtual routing, and segmentation. Other guidance includes scrubbing data prior to hitting the cloud as is often the guidance when addressing HIPAA regulations.

  Many of the requirements in GDPR and other regulations and compliance are based on data sovereignty (knowing where the data resides at any given time) and being able to take additional actions, such as deleting, moving, or sanitizing, the data at any moment. These actions require knowing where the data resides. The NPS solution leverages NetApp equipment residing in a colocation facility. The NPS solution has a key advantage when addressing GDPR because the organization's data is not stored in the cloud; it is stored on the equipment in the colocation facility.
- Encryption or tunneling needs:
  - **Data at rest.** The NPS solution leverages the following NetApp ONTAP® built-in security solutions:
    - NetApp Volume Encryption (NVE)
    - NetApp Storage Encryption (NSE)
    - Onboard key manager (OKM): Both NSE and NVE use the onboard key management solution. The encryption keys are stored in the onboard key manager, which keeps track of all the encryption keys used by ONTAP.
    - External key management: The NSE solution can leverage external or onboard key management. In the external key management solution, the authentication key is backed up to an external key manager using the industry standard OASIS Key Management Interoperability Protocol (KMIP).

  Note: Currently, key management is a single-tenant function.

  - **Data-in-flight encryption.** Data-in-flight encryption is typically performed by leveraging IPSec to make sure of end-to-end communications using layer 3 termination points.
  - **Protocol-level encryption.** The use of protocol-level security functions such as signing and sealing capabilities in SMBv3 and CIFS, integrity and confidentiality with NFSv4, and the use of Kerberos (krb5i and krb5p) further aids in maintaining security posture throughout the Data Fabric and NPS solution.

    For more details about securing the NAS data plane, see Secure Unified Authentication.
  - **Secure access and hardening.** The NPS solution leverages ONTAP software, which provides secure access protocols, including SSHv2 and TLS v1.1 and 1.2. In addition, the ONTAP solution continues to leverage and expand on its built-in security functions and hardening schemes.

    For more details about securing ONTAP, see Security Hardening Guide for NetApp ONTAP 9.
  - **Third-party encryption.** Third-party encryption solutions may also be leveraged to adhere to security needs. Commonly used solutions in NPS include Bitlocker with iSCSI LUNs, which provides data-at-rest and data-in-flight encryption, and SQL transparent data encryption (TDE) for SQL Server, Azure SQL database, and data warehouse data files. TDE provides real-time I/O encryption and decryption of data and log files, providing a key data-at-rest solution.

    For more details regarding TDE, see Transparent Data Encryption.
  - **International Traffic in Arms Regulations (ITAR) boundaries.** ITAR has strict requirements in addition to export controls.

  For more details about ITAR and AWS GovCloud (U.S.) region, see Maintaining U.S. ITAR Compliance.

  - **Security assurance.** Security assurance remains applicable regardless of architecture. Accreditation, third-party testing, and validation continue to provide the posture and rigidity of the security solution.

    For a list of NetApp product security certifications, see NetApp Product Security Certifications.
  - **Physical and operational security.** Leveraging the NPS solution provides organizations with the valuable addition of physical security because the colocation facility provides it through the use of its facility to install and maintain equipment. In addition, operational security is added through the use of secure access protocols in the cloud architecture.
  - **Cloud network security.** Security in the cloud is leveraged through secure access, the aforementioned secure protocols, data-at-rest and data-in-flight encryption options, and the inherent capabilities of the cloud providers.
  - **Private network connectivity (Direct Connect and ExpressRoute).** A key component of the NPS solution is its ability to leverage connectivity capabilities directly to the cloud through physical cross-connects using Direct Connect and ExpressRoute. They physically connect from the dedicated racks/cages, cross-connect to cloud exchange, and then connect through clouds and use cloud exchange APIs to tie to circuits and VLANs.
  - **Segmentation or tenant isolation.** Segmentation and isolation are provided through technologies, including but not limited to VLANs, IP spaces, and VRFs.
  - **Physical security.** The colocation facilities use physical security controls, including security guards, gates, locked door access, badge readers, and biometrics.
  - **Operational security.** In addition to secure capabilities, colocations provide the added value of availability through the use of redundant power and connectivity, including N+2 power and a myriad of heating and cooling capabilities.

Note that NPS is extending the traditional and next-generation data center to the colocation. This approach provides organizations with their own equipment and rack space in a dedicated facility and provides the option for them to manage the equipment or leverage a managed service provider to facilitate operations.

As previously mentioned, the NPS solution, regardless of provider, follows a shared responsibility model. Therefore, customers are responsible for security in the cloud, including but not limited to security for the following items:

- Customer data
- Platforms, applications, and identity and access management (IAM)
- Operating system (OS), network, and firewall configuration
- Client-side data (including encryption)
- Server-side data (including encryption)
- Transport data (network traffic)

The provider is typically responsible for the security of the cloud, which usually includes storage and compute resources, database, and networking resources.

For more details regarding the shared responsibility models, reference the respective providers as follows:

- Amazon Web Services Shared Responsibility Model
- Microsoft Azure Shared Responsibility Model
- MS Azure Security Response in the Cloud

3.1 Data-at-Rest Encryption

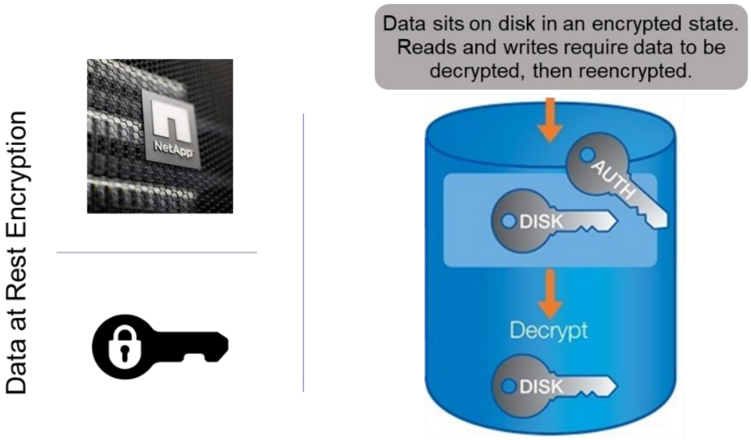
The NetApp solutions that allow data-at-rest encryption are NSE and NVE. NSE is configured to use FIPS140-2 level 2 self-encrypting drives to facilitate compliance and spares return by enabling the protection of data at rest through AES 256-bit transparent disk encryption. The drives perform all of the data encryption operations internally, including encryption key generation.

NVE is a software-based, data-at-rest encryption solution that is available starting with ONTAP 9.1 management software. NVE enables ONTAP to encrypt data (using AES-256 bit encryption) per volume for granularity and to have that data be stored on disk without requiring self-encrypting drives.

For more details regarding the data-at-rest encryption solutions, see the NSE and NVE Datasheet.

Figure 2 illustrates the data-at-rest encryption construct.

Figure 2) Data-at-rest encryption.


Data at Rest Encryption
NetApp
Data sits on disk in an encrypted state. Reads and writes require data to be decrypted, then reencrypted.
AUTH
DISK
Decrypt
DISK

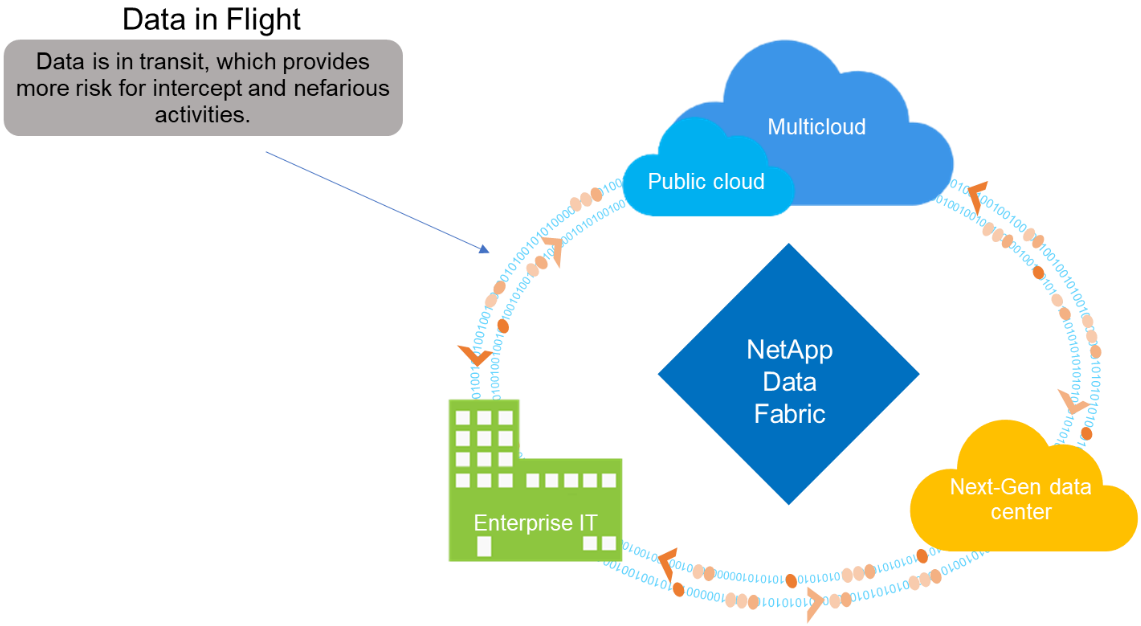
3.2 Data-in-Flight Encryption

The industry-standard IPSec secure encryption protocol is most often invoked to establish encryption or protection for data in flight. When leveraging the IPSec or advanced protocol solutions, the following additional equipment or protocols are needed:

- Layer 3 switch
- Router/firewall: Leverage routers to perform IPSec. Note that this approach works with AWS, but not with Azure (express route). IPSec and its capabilities and extensivity are cloud dependent. In addition, leveraging an IPSec tunnel might have an impact on traffic. This impact is largely dependent on the hardware being used, crypto offload capabilities, and the hardware efficiency itself. Higher end security appliances and routers have fewer performance and throughput impacts, and thus lower end appliances and routers have more of an impact. In testing we have seen ~2ms of latency and the possibility to reduce overall throughput. Testing IPSec in your environment to fully understand the impacts prior to instantiating in production is always recommended.
- NFSv4 (authentication)
- Bitlocker is often used with Windows host and iSCSI LUNs. Note that there is a performance impact on storage efficiency, and therefore testing the impact of leveraging such tools/solutions prior to implementing in production is always recommended.
- SMBv3 (3.1)

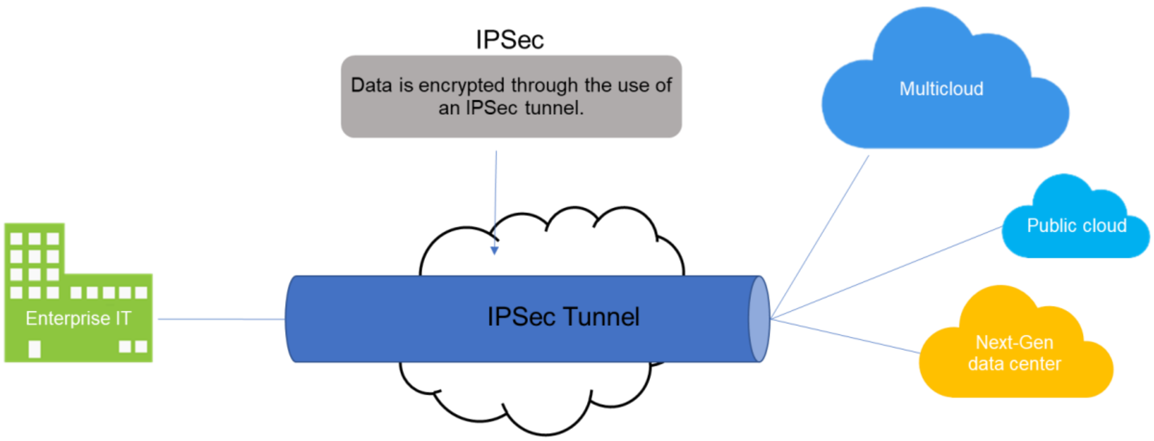
Figure 3 illustrates the data-in-flight encryption construct.

Figure 3) Data-in-flight encryption.



It is key to understand the IPSec construct and the recommendation for leveraging devices to establish an IPSec tunnel to provide encryption means from tunnel endpoints (routers/layer 3 switches), as shown in Figure 4.

Figure 4) IPSec tunnel encryption.



The nature of IPSec provides a means to protect and transport data in a secure manner at the network layer. Because the IP protocol itself does not have built-in security, the IPSec protocol is a way to add security to the IP protocol by addressing the following key functions:

- **Confidentiality.** IPSec leverages encryption to make sure that only the sender and receiver of a particular set of data are able to read it.
- **Integrity.** To make sure that data is not tampered with or modified during transit, IPSec leverages hashing to make sure that the sender and receiver can both verify that the values of the received data are the same and in turn validate that the data has not changed.

- **Authentication.** To make sure that the sender and receiver are talking to their intended recipient, the authentication process invokes methods to validate senders and receivers.
- **Antireplay.** Miscreants sometimes try replay attacks by capturing and resending packets between a sender and receiver. Due to the use of sequence numbers in TCP leveraged by IP, IPSec does not allow for the use of duplicate packets.

Leveraging these details, IPSec enables two or more peers to negotiate and perform authentication and encryption tasks, leverage key exchanges, and secure hashing and encryption algorithms to provide a secure channel for data to be sent from a source to a destination.

Conclusion

The NPS solution provides organizations with an agile and flexible cloud-connected storage solution. The many use cases for NPS further define the myriad of possibilities and capabilities required for businesses today. The NPS solution has the ability to extend an organization's data security solutions and address GRC and encryption needs.

NPS enhances organizations' posture and security practices by taking advantage of the built-in security functions and practices of the solution. In addition to allowing an organization to bring traditional data centers and new architectures into the unified data fabric, enabling the business to move, store, and manage data across flash, disk, and cloud resources in a unified manner, the NPS solution continues to inherently address the challenges of today through its unique and hybrid approach of maintaining the ownership and use of an organization's data management and storage equipment while securely deploying it in a robust and vetted colocation environment.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- NetApp Private Storage
  https://cloud.netapp.com/netapp-private-storage
- NetApp Private Storage for the Cloud
  http://www.netapp.com/us/products/cloud-storage/private-storage-cloud.aspx
- AWS Shared Responsibility Model
  https://aws.amazon.com/compliance/shared-responsibility-model/
- MS Azure Shared Responsibility Model
  http://aka.ms/sharedresponsibility

Version History

Version	Date	Document Version History
Version 1.0	November 2017	Initial release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Trademark Information