White Paper: **June 2022**

Meeting SWIFT CSCF v2022 Requirements with NSX Firewall

vmware®

Table of contents

In 2018, SWIFT announced its Customer Security Controls Framework (CSCF), a set of mandatory security controls for all users of the secure financial messaging services. Since then, the SWIFT CSCF has gone through multiple updates, the latest one being CSCF v2022. While the controls are intended to improve security and reduce risk, installing and maintaining these controls can be cumbersome and time consuming depending on the technical solutions chosen. This white paper demonstrates how organizations can simplify CSCF compliance with NSX Firewall.

The Traditional Approach

SWIFT CSCF requires organizations to segment SWIFT-related workloads from other workloads on the network. Unfortunately, the traditional approach to network design poses a challenge. In many enterprises, network design puts web servers on one VLAN, databases on another VLAN, and business-logic (for example, payment processing) on a third VLAN (and so on). It is impossible to cleanly cordon off a SWIFT application that has workloads on each of the three VLANs with a hardware firewall appliance.

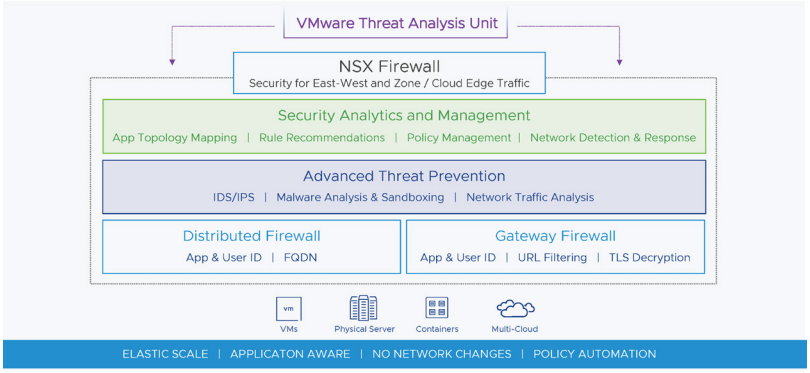
Organizations can address this problem by creating a new VLAN that contains all the workloads for the SWIFT application. However, this requires network architecture changes that depend on heavy coordination between the network and security teams. In addition to the potential re-assignment of IP addresses for some workloads, network downtime may be required. These deployment projects can take weeks or even months.

Fortunately, VMware NSX Firewall can simplify this task.

Introduction to VMware NSX Firewall

VMware NSX Firewall comes in two flavors. While they share code and capabilities, the two firewalls are not identical. One is designed to primarily handle east/west traffic and the other is designed to be an edge firewall.[1] Together, the firewalls deliver consistent protection across your entire infrastructure.

NSX Firewall: Modern Network Defense



1. Edge firewalls handle traffic coming in/out of a demarcated environment. See Internal Firewalls for Dummies Guide for additional discussion on traffic and firewall types.

The VMware NSX Distributed Firewall[2] is a software-defined Layer 2-7 firewall enabled at each workload to segment east-west traffic and block lateral movement of threats. The NSX Distributed Firewall is purpose-built to secure multi-cloud traffic. It provides stateful firewalling delivered as software and distributed to each host. With complete visibility into applications and flows, the Distributed Firewall delivers security with policy automation that's linked to the workload lifecycle.

The NSX Distributed Firewall is complemented by the VMware NSX Gateway Firewall[3] , which is a software-only, Layer 2-7 firewall deployed at zone boundaries. The NSX Gateway Firewall assists the Distributed Firewall in extending protection to physical workloads, thus enabling unified security across physical and virtual workloads in private and public clouds.

Both firewalls include Advanced Threat Prevention capabilities such as IDS/IPS, network sandbox, behavior-based network traffic analysis, and network detection and response.

Key Capabilities of the NSX Distributed Firewall

The NSX Distributed Firewall includes a number of capabilities that help facilitate SWIFT CSCF compliance.

Micro-segmentation

The NSX Distributed Firewall enables micro-segmentation, which reduces the attack surface with fine-grain controls of traffic flow between workloads. The Distributed Firewall isolates and segments resources regardless of the underlying physical network. Its distributed architecture supports stateful network traffic inspection and policy enforcement on a per-workload level. Thus, you can gain visibility of traffic and easily create virtual security zones in minutes with no changes to your network by defining them entirely in software. There is no need to deploy discrete appliances or hairpin traffic.

Because of the Distributed Firewall's micro-segmentation capabilities, no network changes are needed to segment the SWIFT application from other applications, and no IP addresses need to be reassigned. A security tag (for example, SWIFT-APP) is assigned to all the workloads belonging to the application. In the simplest case, communication is only allowed between workloads that have the SWIFT-APP tag. (This process is no different that segmenting any other application using NSX Distributed Firewall.) However, you can go further and micro-segment within the application—for example, by disallowing communication between the web and database tiers.

2. NSX Distributed Firewall
3. NSX Gateway Firewall

User-ID based firewalling

Users typically have different access rights to applications and resources based on their role. The Distributed Firewall's identity-based firewalling capability seamlessly integrates with Active Directory (AD) to enable user-specific security policies. Admins can use the Distributed Firewall to control user access to resources based on their Active Directory groups and identity.

Advanced Threat Prevention

Advanced Threat Prevention (ATP)[4] enables inspection of permitted traffic for the SWIFT application. ATP prevents lateral movement of attackers—even if one of the workloads in the SWIFT application is compromised, the attacker is unable to move beyond the compromised workload. VMware's ATP incorporates multiple detection techniques and includes logic that combines information from all of these:

- Detection technologies
  - Distributed IDS/IPS
  - Network sandbox
  - Network traffic analysis
- Network detection and response
  - Aggregation, correlation, and context engines
  - Including the ability to pull context from sources outside of NSX

Each technology has its own role to play, yet they all work together to provide a cohesive defensive layer, as described below.

Distributed IDS/IPS

Distributed IDS/IPS is a signature-based intrusion detection/prevention system. This technology inspects all traffic that enters the network, detecting and preventing known threats from gaining access to the network, critical systems, and data. IDS/IPS looks for known malicious traffic patterns to hunt for attacks in the traffic flow. When it finds an attack, the IDS/IPS generates an alert, which is logged for post-incident investigation. Depending on administrator configuration, the IDS/IPS can also block an attack.

Distributed IDS/IPS is co-located with the workload to optimize traffic flow. Because it's workload-aware, the IDS/IPS only applies the signatures that relate to the workload, thereby reducing detection effort and the possibility of false positives. These same benefits apply to virtual patching.[5] As an intermediate policy enforcement layer between attackers and unpatched vulnerabilities, the distributed IDS/IPS applies workload-applicable signatures to prevent a vulnerability from being exploited while minimizing false positives and improving throughput.

4. Advanced Threat Prevention with VMware NSX Distributed Firewall
5. Virtual Patching with VMware NSX Distributed IDS/IPS

Network Sandbox

The network sandbox is a secure isolation environment designed to detect malicious artifacts in the data center. The network sandbox analyzes the behavior of objects, such as files and URLs, to determine if they are benign or malicious. Because it is not reliant on signatures, the sandbox can detect novel and highly targeted malware that has never been seen before.

VMware uses the most advanced method of sandboxing available: Full-system Emulation (FUSE)-based sandboxing. FUSE sandboxes emulate the entire hardware—CPU, memory, and I/O devices—enabling the sandbox to see everything the malware is doing. The VMware FUSE sandbox can identify objects with novel exploits, malicious websites, command and control servers, and malware distribution points. Security analysts can study malware and its operation and trigger prevention procedures and provide security alerts and data to other tools. Because the FUSE sandbox emulates everything, it's much more difficult for cybercriminals to evade.

VMware's implementation of sandboxing applies machine learning (ML) to malicious behavior and malware samples, to automatically create classifiers that recognize malicious network behaviors and IDS/IPS signatures. These classifiers and signatures are pushed out to all NSX deployments, thereby continuously increasing the overall efficacy of VMware's ATP.

Network Traffic Analysis

Network traffic analysis (NTA) looks at network traffic and traffic flow records using ML algorithms and advanced statistical techniques to develop a baseline of normal activities. With this foundation, NTA can identify protocol, traffic, and host anomalies as they appear. Additional ML and rule-based techniques help determine if the anomaly is malicious and keep false positives to a minimum. Like Distributed IDS/IPS, NTA is co-located with the workload to enable efficient and thorough analysis of east-west network traffic.

Network Detection and Response

VMware's network detection and response (NDR) consists of aggregation, correlation, and context engines that condense massive amounts of network data down to a handful of intrusions along with their contextual information. The aggregation engine collects signals from various detection technologies and determines whether they are malicious or benign. The correlation engines combine multiple related alerts into a single intrusion, while the context engines add useful context based on data from sources inside and outside of NSX. Armed with this information, security teams can quickly understand the scope of an attack, zero in on real threats, and focus their attention on mitigation and remediation before damage can be done.

Key Capabilities of the NSX Gateway Firewall

The NSX Gateway Firewall provides traditional Layer 2-7 firewall capabilities. The Gateway Firewall filters traffic in a stateful manner, provides network segmentation and includes enhanced security functionalities and traffic flow management capabilities. It is ideal for protecting physical workloads in the private cloud, where it doesn't require access to the OS or hypervisor.

The NSX Gateway Firewall also offers:

- URL filtering to exclude communication with known malicious sites.
- User identity-based access controls to ensure that people access only the applications and resources they need to get their jobs done.
- ATP capabilities to identify threats and block attacks, including IDS/IPS and malware detection that's integrated with network sandboxing.
- Full TLS decryption
- Site-to-site VPN

The Gateway Firewall can serve as a private cloud zone firewall (a firewall at the data center perimeter, between the edge and the internal firewalls). For CSCF compliance, the Gateway Firewall can be used at the edge of the SWIFT environment, where the SWIFT environment connects to the rest of the corporate infrastructure.

NSX Manager

A key component of the NSX architecture, NSX Manager provides a graphical user interface and a REST API to manage all of the VMware NSX infrastructure. Thus, it provides a unified management interface for both the Distributed and Gateway Firewalls. NSX Manager also enables role-based access control (RBAC), which enables you to restrict system access to authorized users based on their roles. Users are assigned roles and each role has specific permissions.

SWIFT CSCF Compliance with NSX Firewall

The capabilities provided by the NSX Firewall help address a number of CSCF requirements,[6] as outlined in the following chart.

6. SWIFT Customer Security Controls Framework v2022

	Requirement	Control objective	NSX Firewall capabilities
1.1	SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	Micro-segmentation (Distributed Firewall); Segmentation (Gateway Firewall)
1.2	Operating System Privileged Account Control	Restrict and control the allocation and usage of administrator-level OS accounts.	User-ID based firewalling (Distributed Firewall); RBAC (NSX Manager)
1.3	Virtualization Platform Protection	Secure the virtualization platform and virtual machines (VMs) that host SWIFT-related components to the same level as physical systems.	Micro-segmentation, ATP (Distributed Firewall)
1.4	Restriction of Internet Access	Control/Protect Internet access from operator PCs and systems within the secure zone.	Segmentation (Distributed Firewall); Traffic filtering, URL filtering (Gateway Firewall)
1.5A	Customer Environment Protection	Ensure the protection of the customer's connectivity infrastructure from external environment and potentially compromised elements of the general IT environment.	Micro-segmentation, ATP (Distributed Firewall); Segmentation, ATP (Gateway Firewall)
2.1	Internal Data Flow Security	Ensure the confidentiality, integrity, and authenticity of application data flows between local and SWIFT-related components.	Micro-segmentation (Distributed Firewall); Micro-segmentation in a container environment (Distributed Firewall Integration with Antrea[7])
2.2	Security Updates	Minimize the occurrence of known technical vulnerabilities on operator PCs and within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.	ATP (Distributed Firewall); ATP (Gateway Firewall)

7. Connect and Secure your Apps with Antrea and VMware NSX-T 3.2

	Requirement	Control objective	NSX Firewall capabilities
2.3	System Hardening	Reduce the cyberattack surface of SWIFT-related components by performing system hardening.	Micro-segmentation, ATP (Distributed Firewall)
2.4A	Back Office Data Flow Security	Ensure the confidentiality, integrity, and mutual authenticity of data flows between local or remote SWIFT infrastructure components and the back-office first hops they connect to.	Micro-segmentation, micro-segmentation in container environments (Distributed Firewall); Site-to-site VPN (Gateway Firewall)
2.5A	External Transmission Data Protection	Protect the confidentiality of SWIFT-related data transmitted or stored outside of the secure zone as part of operational processes.	Micro-segmentation, segmentation (Distributed Firewall)
2.6	Operator Session Confidentiality and Integrity	Protect the confidentiality and integrity of interactive operator sessions that connect to the local or remote (operated by a service provider) SWIFT infrastructure or service provider SWIFT-related applications.	User ID-based Firewalling (Distributed Firewall)
2.7	Vulnerability Scanning	Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results.	Micro-segmentation (Distributed Firewall); Security Tags (created by VMware Carbon Black[8])
2.8A	Critical Activity Outsourcing	Ensure the protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.	Security Tags for policy specification, micro-segmentation (Distributed Firewall); Segmentation (Gateway Firewall)
2.9	Transaction Business Controls	Ensure outbound transaction activity within the expected bounds of normal business.	Segmentation (Distributed Firewall); Policy management (NSX Manager)

8. VMware Carbon Black Cloud Workload

	Requirement	Control objective	NSX Firewall capabilities
2.10	Application Hardening	Reduce the attack surface of SWIFT-related components by performing application hardening on the SWIFT-compatible messaging and communication interfaces, the SWIFT connector, and related applications.	Micro-segmentation, ATP (Distributed Firewall)
2.11A	RMA Business Controls	Restrict transaction activity to validated and approved business counterparties.	Traffic filtering (Gateway Firewall)
5.1	Logical Access Control	Enforce the security principles of need-to-know access, least privilege, and separation of duties for operator accounts.	User ID-based Firewalling (Distributed Firewall); RBAC (NSX Manager); Logs, reports (vRealize Log Insight[9])
5.4	Physical and Logical Password Storage	Protect physically and logically the repository of recorded passwords.	User ID-based Firewalling (Distributed Firewall)
6.1	Malware Protection	Ensure that local SWIFT infrastructure is protected against malware and act upon results.	ATP (Distributed Firewall)
6.4	Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.	ATP (Distributed Firewall); vRealize Log Insight
6.5A	Intrusion Detection	Detect and contain anomalous network activity into and within the local or remote SWIFT environment.	ATP (Distributed Firewall); ATP, TLS Decryption (Gateway Firewall)

Meeting SWIFT CSCF requirements doesn't have to necessitate rearchitecting the network or significant downtime. NSX Firewall reduces hardware dependency and simplifies security posture enforcement required by CSCF. For more information, visit NSX Distributed Firewall and NSX Gateway Firewall.

9. vRealize Log Insight

Item No: vmw-wp-meeting-swift-cscf-requirements-v2 6/22