SWIFT MANDATORY AND ADVISORY SECURITY CONTROLS

Take a Bite Out of the Updated SWIFT Customer Security Controls Framework with Palo Alto Networks

Successful cyberattacks against multiple financial institutions came to light in 2016, resulting in multiple instances of fraudulent fund transfers over the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. As part of an effort to enhance the cybersecurity of the entire ecosystem, members of SWIFT were required to annually self-attest to an initial set of mandatory cybersecurity controls by the end of 2017. Furthermore, a number of advisory security controls were provided as best practices to improve overall cyber hygiene across the SWIFT ecosystem. For 2019, SWIFT updated the Customer Security Controls Framework (CSCF) to include 19 mandatory and 10 advisory controls in recognition of emerging and evolving cyberthreats.

Palo Alto Networks can support your efforts to meet this baseline by contributing to 86% of the updated SWIFT mandatory and advisory security controls. In many cases, the capabilities of the Security Operating Platform® exceed the SWIFT CSCF v2019 controls and can provide even better security outcomes. By incorporating the SWIFT controls into your cybersecurity program and leveraging Palo Alto Networks products accordingly, you can put your financial institution's cybersecurity posture well on the way to meeting the revised SWIFT CSCF.

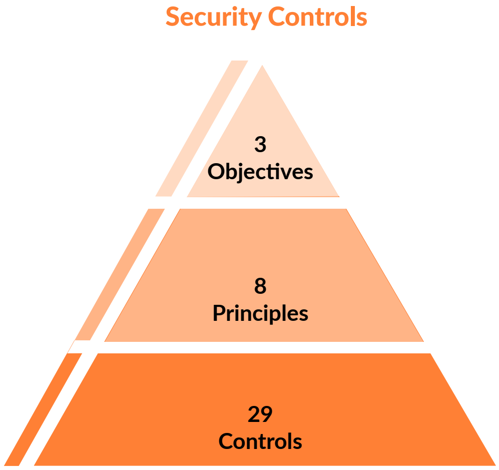
Introduction

SWIFT announced its Customer Security Programme (CSP) in 2016 after a series of successful attacks that bypassed local security measures at several SWIFT member institutions. These attacks occurred across multiple countries and continued well into 2018. The most highly publicized incident, at a bank in Bangladesh, resulted in fraudulent fund transfers of US$81 million initiated through the SWIFT network. Although the SWIFT environment itself has not been compromised in any of these attacks, SWIFT established the CSP as an industry cooperative to reinforce and safeguard the security of the entire ecosystem. One aim of this program is to enhance security guidelines and provide audit frameworks for all members of the SWIFT community.

The first version of the SWIFT CSCF, published in early 2017, prescribed 16 mandatory and 11 advisory controls as a security baseline for the local environments of its member institutions. In recognition of the evolving threat landscape and additional technology adopted by the financial services industry, SWIFT published the CSCF v2019, which now includes 19 mandatory and 10 advisory controls. The mandatory controls set a realistic goal for near-term, tangible security gains and risk reduction to which SWIFT members must self-attest by the end of 2019. In the CSCF v2019, three advisory controls from 2017 have been promoted to mandatory, and two brand-new advisory controls on virtual machines and application hardening have been introduced.

SWIFT Customer Security Controls Framework

The 19 mandatory controls establish a security baseline for all members of the SWIFT cooperative that must be implemented across their local SWIFT infrastructure. The 10 advisory controls are recommended as best practices to complement the security baseline for further improvements in cyber hygiene. The mandatory and advisory controls are in line with existing information security guidelines or standards, such as NIST, PCI DSS, and ISO/IEC 27002. The entire set of 29 controls falls under three overarching objectives—Secure Your Environment, Know and Limit Access, and Detect and Respond—and can be broken down into eight principles (see figure 1).



SWIFT Customer Security Controls Framework

Secure Your Environment	1. Restrict internet access
	2. Protect critical systems from general IT environment
	3. Reduce attack surface and vulnerabilities
	4. Physically secure the environment
Know and Limit Access	5. Prevent compromise of credentials
	6. Manage identities and segregate privileges
Detect and Respond	7. Detect anomalous activity to system or transaction records
	8. Plan for incident response and information sharing

Figure 1: **SWIFT Customer Security Controls Framework**[1]

In many instances, security and compliance teams have had to go above and beyond the minimum industry regulations to establish security architectures that effectively address modern and emerging threats and more closely align with their own institutions' risk tolerances. The same approach may also apply to the SWIFT mandatory security controls, supplemented with implementation of the advisory controls or other additional measures deemed necessary by a given financial institution.

Although no single vendor or offering can deliver full compliance with the entire SWIFT CSCF, financial institutions would be well-served by products and processes that address multiple requirements, ideally in a tightly integrated manner. Today's evolving and emerging threats require a multilayered approach to cybersecurity, based on security enforcement points that natively integrate and share threat information across the entire environment. In other words, if a threat is detected in one location, such as an endpoint, the ideal approach must work to prevent it everywhere—that is, on the network and in the cloud.

Palo Alto Networks Security Operating Platform

The Palo Alto Networks approach to security focuses on prevention rather than detection. The key elements of this approach are to provide visibility, reduce the attack surface area, prevent all known threats, and detect and prevent new threats. The Palo Alto Networks Security Operating Platform® is a tightly integrated system of components and services, including a partner ecosystem, that delivers consistent security across networks, endpoints, and clouds. The intelligence derived from one component benefits the others across the enterprise.

[1] "Customer Security Programme," SWIFT, accessed November 21, 2019, https://www.swift.com/myswift/customer-security-programme-csp_/security-controls/2019.

Palo Alto Networks has built a platform that uses consolidated threat intelligence, automation, analytics, machine learning, and AI to offer comprehensive coverage across the enterprise environment, including the cloud. Key attributes are the ability to protect consistently everywhere, automate tasks for efficiency, and offer visibility into network data regardless of location. Benefits of this approach include lowering mean time to respond (MTTR) and mean time to detect (MTTD), reducing risk and increasing efficiency for your teams.

In the next two sections, we will review the applicability of the Security Operating Platform to the relevant SWIFT mandatory and advisory controls.

Meet and Exceed SWIFT Mandatory Controls

Through the capabilities of various components of the Security Operating Platform, an organization can meet or exceed the minimum security baseline for 16 of the 19 SWIFT mandatory controls.

1. Restrict Internet Access & Protect Critical Systems from General IT Environment

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.

In short, this calls for effective network segmentation of the local SWIFT infrastructure from the rest of the IT environment. By compartmentalizing the SWIFT elements, a compromise elsewhere in an institution's environment would pose minimal risk to SWIFT operations. Think of this as establishing a Zero Trust network for the local SWIFT infrastructure. Palo Alto Networks Next-Generation Firewalls may serve as segmentation gateways to safely enable desired applications across zones, into or out of the local SWIFT environment. Lateral movement by malicious entities or even unauthorized insiders is restricted accordingly.

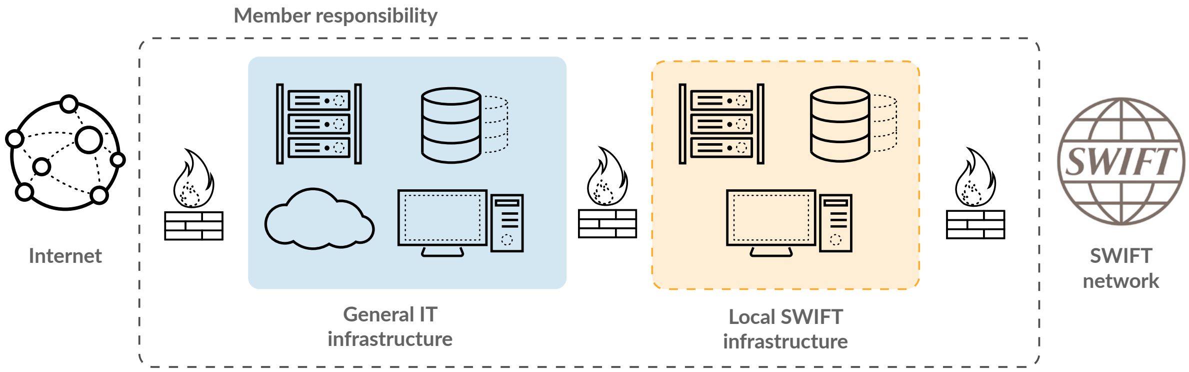


Figure 2: Network segmentation of local SWIFT components

1.2 Operating System Privileged Account Control: Restrict and control the allocation and usage of administrator-level operating system accounts.

The principle of least privilege should be applied to ensure administrator-level access is limited to personnel who need it for their job functions. Moreover, administrative privileges should be tied to specific system accounts and user IDs. Next-Generation Firewalls may be deployed as multi-factor authentication (MFA) gateways to require additional credentials from administrative users. This policy-based approach occurs at the network layer instead of on a per-application or per-server basis to accommodate even legacy resources that do not support MFA. Consequently, even stolen administrator-level credentials are no longer sufficient to impersonate valid actors.

2. Reduce Attack Surface and Vulnerabilities

2.1 Internal Data Flow Security: Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.

With complete visibility into network activity, the Next-Generation Firewall substantially reduces the attack surface by enabling only the desired applications, limiting dangerous file types and blocking known threats via the Threat Prevention subscription. WildFire® malware prevention service quickly identifies unknown threats and makes them known, delivering new protection to the entire Security Operating Platform in as few as five minutes. Traps™ endpoint protection, meanwhile, protects operator PCs against malware and exploits. For even greater protection of the data flow, the GlobalProtect™ agent can be deployed on operator PCs to validate local host security configurations and, if satisfactory, establish an IPsec VPN for privacy.

2.2 Security Updates: Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.

Where timely software patching is not possible for whatever reason, Traps can effectively prevent exploits and malware from compromising laptops, PCs, and servers. Traps takes a unique, multi-method approach to preemptively block both known and unknown threats, even for unpatched or unpatchable systems. Legacy systems that are still active, such as aging ATMs or servers still running Windows® XP, can be protected from malware and exploits by Traps. In the specific case of any unpatched local SWIFT components, they can be protected from vulnerabilities with Traps. This can serve as a mitigating control until the appropriate patches are ultimately applied.

2.3 System Hardening: Reduce the cyber attack surface of SWIFT-related components by performing system hardening.

To complement system hardening, the Next-Generation Firewall can limit data flow to only relevant and desired applications by virtue of App-ID™ technology, which can recognize traffic by the actual application protocol instead of just the TCP/UDP port numbers. By establishing security policies with this granular level of control, organizations can further minimize the available attack surface of even hardened systems.

2.6 Operator Session Confidentiality and Integrity: Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.

In an ideal scenario, all dedicated operator endpoints would be located in the separate, protected, local SWIFT environment, eliminating the exposure of that traffic flow to the rest of the IT environment. However, this may not be cost-effective or operationally practical for a number of reasons, including geographic separation.

With the local SWIFT infrastructure segregated as prescribed by Mandatory Control 1.1, that same Next-Generation Firewall can limit remote operator access to a set of specific administrative users with User-ID™ technology, and then, by virtue of deep visibility with App-ID, further limit that access to only particular applications. User-ID enables the Next-Generation Firewall to identify all users on the network and enforce security policy based on user group membership. App-ID is a traffic classification system that identifies applications based on their behavioral characteristics and relative risk. The Next-Generation Firewall can also enforce policy based on specific App-IDs. Threat Prevention and WildFire subscriptions add greater protection against intrusion and unknown malware.

You can use GlobalProtect™ network security for endpoints to establish a secure SSL/IPsec VPN connection to the Next-Generation Firewall to further protect the contents of operator sessions from outside the local SWIFT environment. GlobalProtect collects device information, such as OS patch level, anti-malware measures, and disk encryption, that enables the firewall to permit access only when the endpoint is properly configured and secured.

Finally, the integrity of any operator endpoints will benefit from the multiple methods of prevention Traps offers against malware and exploits. See figure 3 for an overview of protecting operator sessions with the Security Operating Platform.

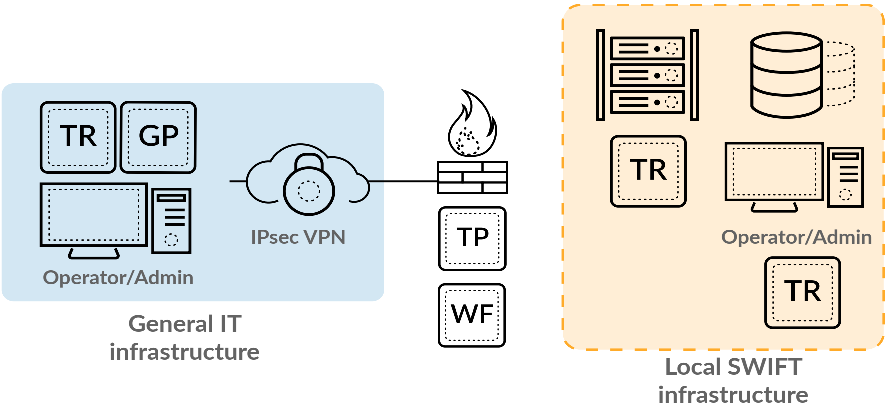


Figure 3: Protecting operator sessions with the Security Operating Platform

2.7 Vulnerability Scanning: Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results.

The Security Operating Platform is not part of the vulnerability scan itself, but various components help prevent discovery and exploitation of vulnerabilities during such exercises by ethical or malicious entities. Traps can prevent fingerprint scanning by exploit kits to restrict attackers' ability to discover operating system and application information. The Next-Generation Firewall with Threat Prevention blocks evasive techniques and attempts to exploit vulnerabilities based on system flaws, buffer overflows, illegal code execution, and other means. WildFire adds further protection against unknown malware.

Should scanning identify vulnerable assets in the environment, Cortex XDR™ by Palo Alto Networks may be used to more closely monitor the assets for specific behavioral indicators of compromise (BIOC), and then to alert and respond when malicious activities begin. In addition to preconfigured BIOC rules with content updates, organizations may add local, customized rules as additional threats are investigated. This additional focus on vulnerable portions of the environment would be appropriate until the vulnerabilities can be permanently addressed.

4. Prevent Compromise of Credentials

4.1 Password Policy: Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.

Although the Security Operating Platform cannot enforce specific password policies, our credential theft prevention capability can stop the submission of corporate login and password information to phishing or other unauthorized websites. This provides an added measure to protect corporate login credentials from a common theft technique.

4.2 Multi-factor Authentication: Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.

As mentioned previously, the Next-Generation Firewall provides a centralized, policy-based MFA framework that can be deployed in front of local SWIFT-related systems. This is achieved by working at the network level in conjunction with authentication and identity management frameworks, such as single sign-on and MFA, and integrating with a number of next-generation identity and access management (IAM) vendors, including Okta, Ping Identity, and Duo Security. This offers the benefits of MFA without any modifications to individual SWIFT-related systems.

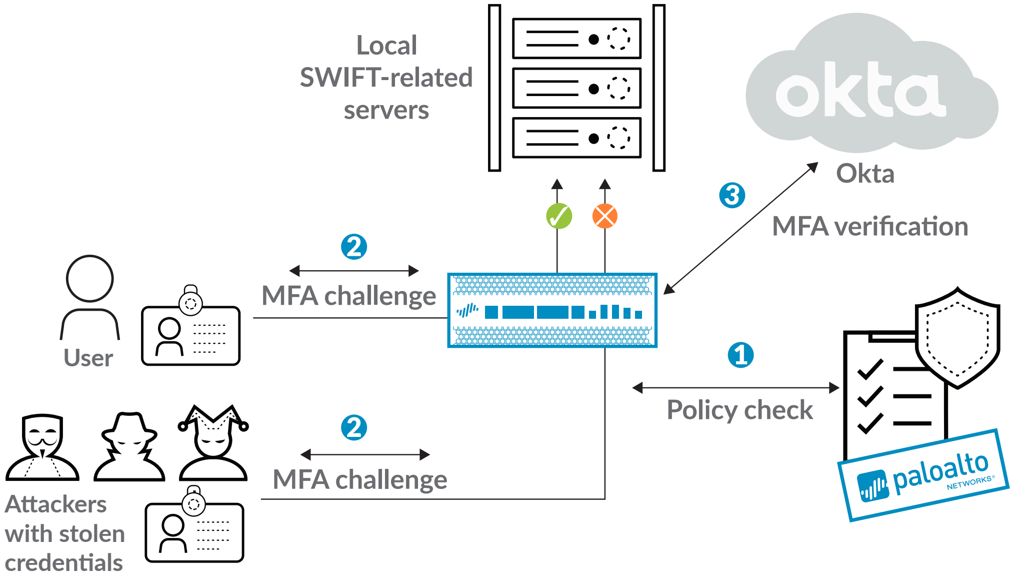


Figure 4: Next-Generation Firewall as an MFA gateway using Okta

5. Manage Identities and Segregate Privileges

5.1 Logical Access Control: Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.

User-based policy controls on the Next-Generation Firewall can include application information for greater context. Organizations can define security policies to safely enable applications based on specific users or groups of users. In other words, you can limit access to particular SWIFT-related applications to only the set of users that require it by taking advantage of our User-ID and App-ID capabilities. This approach is essentially applying the Zero Trust model to the community of users that need access to SWIFT infrastructure. In this fashion, secure access to essential business applications is enabled, but modern malware, targeted attacks, and unauthorized access are stopped.

5.2 Token Management: Ensure the proper management, tracking, and use of connected hardware authentication tokens (if tokens are used).

As part of our MFA gateway functionality, the Next-Generation Firewall supports the use of hardware tokens via RADIUS.

5.4 Physical and Logical Password Storage: Protect physically and logically recorded passwords.

With internal network segmentation in place, access to corporate directories and password repositories can be limited to expected applications and protocols so that unexpected attempts to access those servers by attackers or unauthorized insiders will be blocked. With the Zero Trust model in place, even if malicious actors do somehow access password files, their attempts to exfiltrate that information will also be thwarted.

Additionally, you may use Next-Generation Firewalls at the network edge to prevent credential theft by blocking attempts to submit enterprise login and password information to phishing or unauthorized websites.

6. Detect Anomalous Activity to Systems or Transaction Records

6.1 Malware Protection: Ensure that local SWIFT infrastructure is protected against malware.

At a minimum, SWIFT servers and operator workstations should have Traps for protection against malware and exploits. The Next-Generation Firewalls at the network perimeter and those serving as segmentation gateways internally can run WildFire. Moreover, the Next-Generation Firewalls can also be enabled with Threat Prevention and URL Filtering subscriptions for maximum protection against malware.

In the event malware still finds its way into your environment, Cortex XDR accurately detects threats with behavioral analytics and reveals the root cause to speed up investigations. Tight integration with enforcement points accelerates containment, enabling you to stop attacks before damage is done.

6.2 Software Integrity: Ensure the software integrity of the SWIFT-related applications.

Deploy Traps to protect SWIFT-related servers and workstations from malware and exploits that may attempt to inject malicious code for execution.

6.4 Logging and Monitoring: Record security events and detect anomalous actions and operations within the local SWIFT environment.

The Next-Generation Firewalls at the network perimeter or the internal network have built-in logging and reporting capabilities. Similarly, Traps log data is available for the endpoint perspective. Local monitoring and analysis are possible on the Next-Generation Firewall and through Panorama™ network security management, or they may be handled by a security information and event management (SIEM) product. For even more complete insight into anomalous traffic, Cortex XDR removes security blind spots by stitching together network, endpoint, and cloud data for behavioral analytics using AI, which allows you to quickly identify and eliminate threats.

7. Plan for Incident Response and Information Sharing

7.1 Cyber Incident Response Planning: Ensure a consistent and effective approach for the management of cyber incidents.

Cortex XDR simplifies investigations with automated root cause analysis, coordinates response across all Palo Alto Networks enforcement points, and streamlines behavioral threat hunting. Using Demisto® for security orchestration, automation, and response (SOAR), security teams can execute standardized, automatable playbooks for accelerated incident response that is consistent and repeatable.

Table 1: Mapping of SWIFT Mandatory Controls to Palo Alto Networks Products

Mandatory Controls	Next-Gen Firewall (NGFW)	Cortex
1.1 SWIFT Environment Protection	NGFW, Threat Prevention, WildFire, URL Filtering	Traps
1.2 OS Privileged Account Control	NGFW (MFA gateway)	
2.1 Internal Data Flow Security	NGFW, Threat Prevention, WildFire, GlobalProtect	Traps
2.2 Security Updates		Traps
2.3 System Hardening	NGFW, App-ID	
2.6 Operator Session Confidentiality and Integrity	NGFW, Threat Prevention, WildFire, GlobalProtect, User-ID, App-ID	Traps
2.7 Vulnerability Scanning	NGFW, Threat Prevention	Cortex XDR, Traps
4.1 Password Policy	NGFW	

Table 1: Mapping of SWIFT Mandatory Controls to Palo Alto Networks Products (continued)

Mandatory Controls	Next-Gen Firewall	Cortex
4.2 Multi-Factor Authentication	NGFW (MFA Policy)	
5.1 Logical Access Control	NGFW, User-ID, App-ID	
5.2 Token Management	NGFW	
5.4 Physical and Logical Password Storage	NGFW	
6.1 Malware Protection	NGFW, Threat Prevention, WildFire, URL Filtering	Cortex XDR, Traps
6.2 Software Integrity		Traps
6.4 Logging and Monitoring	NGFW, Threat Prevention, WildFire, URL Filtering	Cortex XDR, Cortex Data Lake, Traps
7.1 Cyber Incident Response Planning		Cortex XDR, Demisto

Meet and Exceed SWIFT Advisory Controls

The capabilities of various components of the Security Operating Platform enable you to meet or exceed nine of the 10 SWIFT advisory controls. As mentioned previously, these are recommended best practices to complement the baseline security required of SWIFT members. The following section discusses the advisory controls where the Security Operating Platform is applicable.

1. Restrict Internet Access & Protect Critical Systems from General IT Environment

1.3A Virtualization Platform Protection: Secure virtualisation platform and virtual machines (VM's) hosting SWIFT related components to the same level as physical systems.

VM-Series Virtualized Next-Generation Firewalls offer equivalent functionality to our hardware-based Next-Generation Firewalls and support both private and public cloud deployments. The VM-Series provides the same deep visibility and granular control found in our hardware Next-Generation Firewalls for any data in the cloud. Traffic flows between applications running on VMs may also be tightly monitored and controlled using User-ID and App-ID context available in the security policy.

2. Reduce Attack Surface and Vulnerabilities

2.4A Back Office Data Flow Security: Ensure the confidentiality, integrity, and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components.

As an example, SWIFT Alliance Access uses IBM Websphere MQ to exchange messages with back-office applications. With complete visibility into network activity, the Next-Generation Firewall can natively recognize and enable MQ as a sanctioned application, limiting dangerous file types and blocking known threats. WildFire quickly identifies unknown threats and makes them known, with new protection delivered to the Next-Generation Firewall in as few as five minutes. Traps protects back-office servers and SWIFT components against malware and exploits. With its components working together, the Security Operating Platform can tightly control and manage traffic to and from SWIFT-related applications, greatly reducing the attack surface.

2.5A External Transmission Data Protection: Protect the confidentiality of SWIFT-related data transmitted and residing outside of the secure zone.

To protect SWIFT-related data leaving the local infrastructure, a Next-Generation Firewall with Threat Prevention and URL Filtering subscriptions can stop traffic to phishing and command-and-control (C2) sites. Our exfiltration protection also includes sinkhole capabilities for outbound traffic destined to malicious domain names. WildFire quickly identifies newly created DNS names that may be used for malicious purposes. Further protection against exfiltration via DNS tunnels is available with our DNS Security service subscription, which applies predictive analytics, machine learning, and automation to block such attacks.

2.8A: Critical Activity Outsourcing: Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.

Deploy a Next-Generation Firewall at the network perimeter for business-to-business connections to any third-party suppliers. Include the use of Threat Prevention and WildFire subscriptions to block anomalous activities and malware from third parties. This same perimeter firewall can also serve as an MFA gateway to challenge third parties for additional credentials before they are permitted to access any of your institution's applications or data.

2.9A Transaction Business Controls: Restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business.

Although some of this involves ensuring appropriate privilege levels within the sanctioned SWIFT-related applications themselves, the Next-Generation Firewall, as described in 2.8A, will help reduce the attack surface available to third parties. By restricting access to a defined set of permissible applications, you give counterparties only the visibility of those resources they require to conduct their normal business. This enforces the principle of least privilege on your third-party partners.

2.10A Application Hardening: Reduce the attack surface of SWIFT-related components by performing application hardening on the SWIFT-certified messaging and communication interfaces and related applications

With the visibility offered by App-ID and Content-ID, the Next-Generation Firewall can inspect and limit traffic to expected application protocols between SWIFT components. More than 3,000 predefined App-IDs exist today, including one for IBM Websphere MQ, which is used for back-office application communications. If desired, organizations can create custom App-IDs for SWIFT messaging applications as well. With tight control over the explicit traffic flows to and from the local SWIFT elements, the attack surface is significantly minimized.

6. Detect Anomalous Activity to Systems or Transaction Records

6.5A Intrusion Detection: Detect and prevent anomalous network activity into and within the local SWIFT environment.

With Threat Prevention, our Next-Generation Firewalls provide integrated and coordinated protection against intrusion, malware, and C2 activities in a single pass, providing high throughput without sacrificing security.

Cortex XDR, our cloud-based detection and response offering, removes security blind spots by stitching together network, endpoint, and cloud data to stop sophisticated threats. Using behavioral analytics, it can identify unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source by detecting behavioral anomalies that may be indicative of attacks.

7. Detect Anomalous Activity to Systems or Transaction Records

7.3A Penetration Testing: Validate the operational security configuration and identify security gaps by performing penetration testing.

Although Palo Alto Networks does not do actual penetration testing, we can complement this activity with Prisma Cloud, Security Lifecycle Reviews (SLR), and Prevention Posture Assessments (PPA).

Prisma Cloud

Prisma™ Cloud by Palo Alto Networks dynamically discovers cloud resources and sensitive data across Google Cloud Platform (GCP™), Amazon Web Services (AWS®), and Microsoft Azure® in addition to detecting risky configurations and identifying network threats, suspicious user behavior, malware, data leakage, and host vulnerabilities. It eliminates blind spots across cloud environments and provides continuous protection with a combination of class-leading machine learning and the most complete collection of rule-based security policies. This provides protection for any workloads that may reside in your public cloud environment.

Security Lifecycle Review (SLR)

Our Security Lifecycle Review is a cloud-based application that summarizes the security risks your organization faces. You can use SLR reports to assess threat exposure by getting a high-level view of the applications in use on your network (including SaaS applications), the websites your users are accessing, and the types of files they're sharing. SLR reports also outline the vulnerabilities, malware, and C2 infections found on your network and help you to contextualize these findings against industry peers.

Prevention Posture Assessment (PPA)

The Prevention Posture Assessment is a consultative tool designed to expose gaps in your network, cloud, and endpoint security environments. It provides a holistic view of your network, through the lens of the cyberattack lifecycle, by assessing how you are leveraging prevention capabilities throughout each area of architecture. With a better understating of the current state of your network, and with any gaps in your architecture identified, you can then develop a plan to get to the desired future state: a prevention-oriented architecture.

7.4A Scenario Risk Assessment: Evaluate the risk and readiness of the organization based on plausible cyber attack scenarios.

Just like for control 7.3A, the SLR and PPA can provide insight into cybersecurity risks in your environment and complement any risk assessments conducted.

Table 2: Mapping of SWIFT Advisory Controls to Palo Alto Networks Products and Tools

Advisory Control	Next-Gen Firewall (NGFW)	Threat Prevention	Other
1.3A Virtualization Platform Protection	VM-Series, Threat Prevention, WildFire, URL Filtering	Traps	
2.4A Back Office Data Flow Security	NGFW, Threat Prevention, WildFire, App-ID	Traps	
2.5A External Transmission Data Protection	NGFW, DNS Security		
2.8A Critical Activity Outsourcing	NGFW, Threat Prevention, WildFire		
2.9A Transaction Business Controls	NGFW, Threat Prevention, WildFire		
2.10A Application Hardening	NGFW, App-ID		
6.5A Intrusion Detection	NGFW, Threat Prevention	Cortex XDR	
7.3A Penetration Testing			Prisma Cloud, SLR, PPA
7.4A Scenario Risk Assessment			SLR, PPA

Summary

No single vendor or solution can provide full compliance with the SWIFT mandatory and advisory controls. What organizations require instead is a thorough set of policies, processes, and practices, supported by an essential set of technological countermeasures to enforce them. The ultimate goal is not merely to complete the annual SWIFT self-attestation, but rather to improve cybersecurity for the organization, which will benefit the local SWIFT infrastructure as well. In this regard, the Palo Alto Networks Security Operating Platform is invaluable, delivering:

- Definitive least-privileged access control and other essential security capabilities to effectively segment and protect the local SWIFT environment for a Zero Trust network.
- Support for 86% of the SWIFT CSCF v2019, addressing all but four controls. Of these, only one relates to technology (6.3 Database Integrity) while the others pertain to personnel, training, and physical security.
- Capabilities above and beyond the baseline specifications to more thoroughly protect your local SWIFT infrastructure and the remainder of your organization's computing environment from the latest unknown malware and advanced threats.

With the power of the Security Operating Platform, financial institutions can be well on their way to complying with or exceeding the SWIFT mandatory and advisory controls. Beyond merely an exercise in compliance, the prevention philosophy behind the platform will improve your overall cyber hygiene and provide better security outcomes for your organization. The result will be a more secure environment for your financial institution—one in which legitimate traffic is known and limited, with automated security enforcement to detect and address deviations.

For more information about the Security Operating Platform and its component technologies, please visit paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com