Implement Network Segmentation and Encryption in Cloud Environments

Executive summary

Network security is a crucial component for cloud users to configure properly. Historically, network security practices have focused on perimeter security, with few additional restrictions once authenticated to an organization's internal network and the acceptance of unauthenticated and vulnerable "internal" protocols. Over the years, this has changed with the push to adopt Zero Trust (ZT) security principles such as:

- Tying identity information into network requests
- Implementing end-to-end encryption
- Micro segmenting the network

This cybersecurity information sheet (CSI) makes recommendations for implementing these principles in a cloud environment, which can differ from on-premises (on-prem) networks. While on-prem networks require specialized appliances to enable ZT, cloud technologies natively provide the necessary infrastructure and services for implementing these recommendations to varying degrees. This CSI focuses on best practices using features commonly available in cloud environments.

Network encryption

Encrypting data in transit is an integral part of cybersecurity. A well-positioned malicious cyber actor (MCA) may be able to observe network traffic in an attempt to capture sensitive information (such as user credentials) passed over the network either unencrypted or weakly encrypted.

ATT&CK® Tactic	Technique
Credential Access	Network Sniffing [T1040]
Credential Access, Collection	Adversary-in-the-Middle [T1557]

One recommended mitigation to prevent this is to encrypt data in transit using NSA recommended algorithms in the Commercial National Security Algorithm (CNSA) Suite or using National Institute of Standards and Technology (NIST) recommended algorithms. [1], [2]

ATT&CK Mitigation
Encrypt Sensitive Information [M1041]

D3FEND™ Tactic	Countermeasure
Network Isolation	Encrypted Tunnels [D3-ET]

Cloud network traffic can be grouped into two general categories: client connections to the cloud platform and internal cloud traffic between services. The following subsections discuss actions cloud users should take to ensure their data is secure in transit.

Connecting to the cloud

Client connections to the cloud environment must be securely encrypted. Users can access cloud platform application programming interfaces (APIs) through a web browser or a command line interface (CLI). Cloud platforms generally require client connections to be encrypted; however, they may allow clients to use weak algorithms to maintain support for connections from legacy clients. All cloud users should ensure they are connecting to the cloud platform over protocols using CNSA Suite algorithms.

While CNSA Suite 1.0 is the current standard for National Security Systems (NSS), organizations should push to adopt CNSA Suite 2.0 requirements where possible to improve their security posture. [1] NSA selected the algorithms from those chosen by NIST; while use of CNSA algorithms are recommended, organizations that do not own or operate national security systems may use NIST recommended algorithms (preferably those in the Federal Information Processing Standard (FIPS) 140-3) to improve their security posture. [2], [3]

For most application-specific protocols (i.e., above TCP or UDP), NSA and CISA recommend TLS 1.2 or later. This includes any connections from customer applications that interact with the organization's cloud environment. Connections to cloud resources should also always pass over a secure channel. Cloud resources like virtual machines and customer applications deployed in PaaS offerings, are the customer's responsibility to secure. The cloud service provider's (CSP's) security policies will not protect a customer application deployed in the cloud that does not implement encryption.

Organizations can use virtual private networks (VPNs) to connect to the cloud, ensuring that users' traffic to the cloud passes through an encrypted channel. For tunneling general IP traffic (i.e., connecting through a VPN) using commercial components, NSA

and CISA recommend using IPsec VPNs. In particular, IPsec VPN products that have been tested and validated and are on the National Information Assurance Partnership (NIAP) Product Compliant List. TLS-based VPNs lack standardization to objectively measure their assurance, and are currently not recommended for tunneling of general purpose IP traffic. Organizations using this option can configure their cloud tenant to only accept connections from the VPN. Then they can use the VPN to centrally manage access and log and monitor the network traffic, providing an additional layer of security and visibility for the organization into the usage of their cloud tenant. For additional guidance on VPNs see NSA's reports: Selecting and Hardening Remote Access VPN Solutions, Network Infrastructure Security Guide, and Configuring IPsec Virtual Private Networks. [4], [5], [6] Organizations can use VPNs to secure both client connections to the tenant and connections to cloud resources. While they are not the only mechanism for doing this, VPNs are a good option for ensuring consistent enforcement of encryption requirements across the organization.

Private connectivity

CSPs frequently offer private connectivity options. These offerings provide organizations using cloud resources a way to connect to the cloud provider's infrastructure directly over a private network connection rather than over the Internet. This greatly reduces the chances of an MCA being able to sniff an organization's network traffic or target vulnerable protocols for exploitation. These options will vary by CSP, but may include offerings such as direct network connections. Direct network connections allow organizations to connect to the CSP's infrastructure directly or through a third party (i.e., one of CSP's connection partners), rather than connecting over the Internet.

Traffic mirroring

Many CSPs offer a traffic mirroring service, which allows users to duplicate and forward traffic. Defenders can use this service to collect incoming network traffic and perform deep packet inspection to identify potential threats. However, this can also be leveraged by MCAs in their post-exploitation activities. MCAs with enough privileges in the tenant from initial exploitation activities can use these services to collect and exfiltrate data that has been decrypted at the load balancer. [7]

ATT&CK Tactic	Technique
Exfiltration	Automated Exfiltration: Traffic Duplication [T1020.001]

Users deploying applications or running compute instances in the cloud behind a load balancer should be aware of whether the load balancing service uses TLS termination. Organizations should closely monitor usage of traffic mirroring within a cloud tenant to identify malicious usage. NSA has further discussed risks and deployment models for TLS inspection in Managing Risks from Transport Layer Security Inspection. [8]

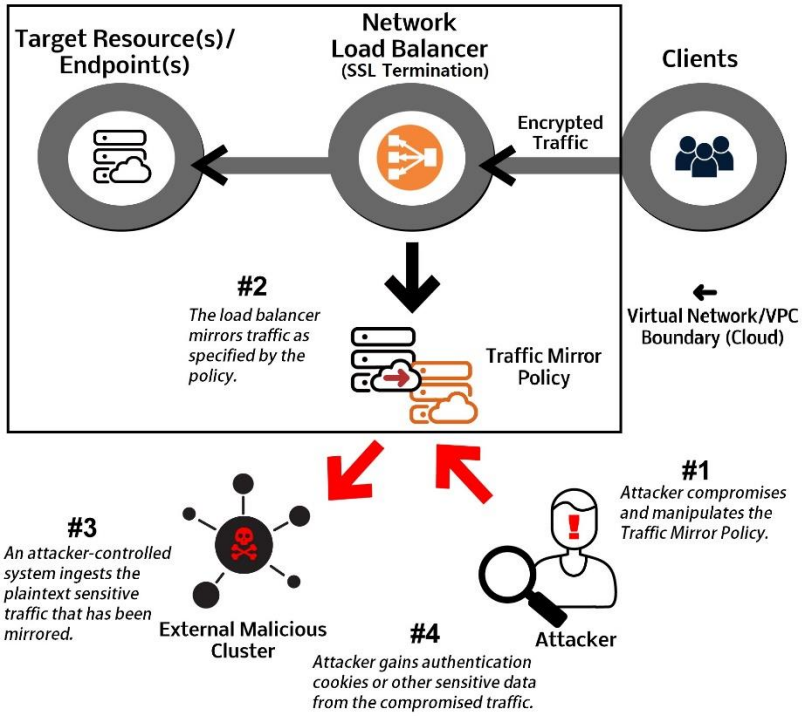


Figure 1: Exfiltration using traffic mirroring example

Backend traffic

While working in the cloud, data will necessarily traverse the CSP's network between services. For example, if a user uploads data to be stored in a cloud storage bucket, encrypted with a customer-managed key, the key management service and the data storage service must communicate to perform this function. Ideally, this traffic should be encrypted and isolated from traffic of other tenants. As these operations are a part of the CSP's environment, cloud users generally do not have insight or control over these processes. Organizations deciding what cloud platform to use can review the CSP's documentation and ask the provider how they protect customer data in their backend, to determine if the CSP's practices fit the organization's needs.

Organizations operating in the cloud should be aware that traffic between customer resources in the cloud does not necessarily stay within the cloud. In some cases, customer traffic may be routed over the Internet, opening it up for inspection or even manipulation by a well-positioned MCA. To mitigate such risks, organizations must

secure traffic between customer resources. Additionally, some CSPs offer private API endpoints that customers can use to ensure that traffic in the virtual enclave to a CSP API will stay within the cloud. Developers writing applications to run in the cloud can use these APIs rather than the usual frontend APIs to allow their applications to connect directly to cloud services rather than be routed back out to the Internet.

If external services need to interact with the application deployed in the cloud, organizations can configure identity-based access policies to restrict access to the application to trusted parties using a policy enforcement point. For more information on this, see CISA's Trusted Internet Connections 3.0: Cloud Use Case report. [9]

Network segmentation

NIST defines network segmentation as splitting a network into subsections where firewalls reject unnecessary traffic for that section. [10] This is a foundational cybersecurity principle, which, when properly implemented, can isolate malicious activities to a limited part of the network and minimize the effect of a breach.

Historically, the focus of network security has been on the perimeter, setting up firewalls to secure an organization's network without placing any additional restrictions once users are authenticated. When using this perimeter-focused approach to network security, MCAs who breach that first line of defense will have access to target user traffic and organization resources, exploiting any vulnerable or unauthenticated network protocols and delivering malicious payloads. In modern cloud environments, there should be more than only a perimeter-focused defense. CSPs should provide a level of isolation between customer tenants; however, the customer is responsible for properly configuring networking within their tenant. Many CSPs offer managed services to enforce this segmentation, such as traffic management, network gateway, and load balancing solutions.

ATT&CK Tactic	Technique
Lateral Movement	Remote Services: Cloud Services [T1021.007]
Lateral Movement	Remote Services: Direct Cloud VM Connections [T1021.008]

At a minimum, resources from different teams should be separated from each other and from tenant administrator groups. This high-level separation is known as "macro segmentation" and is the first step in this process. Any unnecessary network services,

protocols, or ports should be disabled. For example, SSH should be disabled on all cloud compute instances that do not require it, and public IPs should only be configured for production instances that require them. Ideally, only data flow paths necessary for continued normal operations within the environment should be allowed. For example, if two applications deployed in an organization's cloud environment do not need to communicate, no communication path between them should exist. Additionally, if the only communication needed between them is for one to send telemetry data to the other, then that one-way data path should be the only path allowed. This granular segmentation based around approved data ingress and egress points is known as "micro segmentation." This is what organizations should strive for, and it is achievable using cloud native capabilities.

ATT&CK Mitigation
Network Segmentation [M1030]

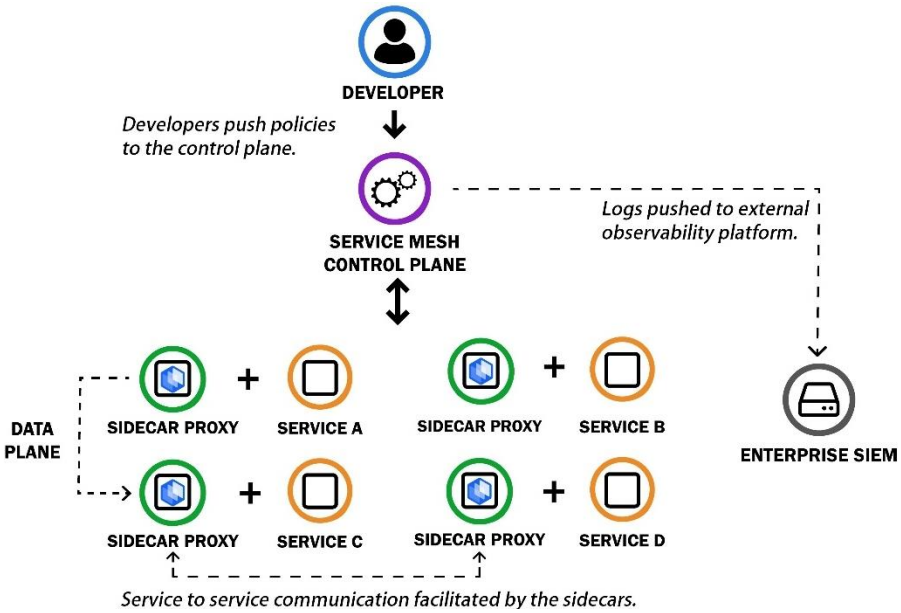
D3FEND Tactic	Countermeasure
Network Isolation	Network Traffic Filtering [D3-NTF]

Typically, CSPs offer users the ability to configure firewall policies and assign them to their virtual compute instances. Users should be aware of what the default rules are and, if needed, set their own default policy to deny all external traffic to the instance. Different CSPs offer different levels of granularity to which policies can be refined. In some cases, general policies can be created for groups of instances and then additional access control policies can be added to individual instances to further refine. When using compute instances in a cloud environment, users should review the CSP's documentation to ensure they understand how traffic is handled and can be restricted to configure this properly.

When developing applications in the cloud, developers can also use a service mesh to help manage and map traffic flows. A service mesh is essentially a web of lightweight proxies that run as sidecars to each micro-service component of an application and manage service-to-service communication. The control plane of the service mesh manages, monitors, and pushes policies out to the sidecar instances. Service meshes typically include monitoring functionality, which can provide developers insight into

normal traffic patterns for a given distributed application. This information can inform policies enforcing encryption between services, authorization policies, and more.

Figure 2: Example of a service mesh



When running large, distributed applications, it can be difficult to keep track of all of the communication paths that are necessary, which can in turn, make it difficult to identify anomalies. Service meshes are useful for such deployments as they simplify service-to-service communications for the developers, facilitate service-to-service encryption for added security, and monitor traffic. This enables developers to implement micro segmentation without breaking services, and it provides detailed metrics that can be passed to anomaly detection services.

Virtual networking

CSPs offer a virtual networking option that allows users to launch cloud resources in a logically isolated virtual network (sometimes referred to as a Virtual Private Cloud or VPC). The specific functionality will vary by provider, but these offerings usually include traffic flow logging, firewalls, troubleshooting and analyzer tools, and private IP subnetting. These services can be leveraged to implement segmentation, as well as additional security and monitoring functionality. Traffic flow logs should be enabled, as they provide useful information for organizations performing threat hunting in their environment. Management privileges should be restricted according to the principle of least privilege, and those with administrator privileges should use phishing-resistant

MFA. For additional guidance see the reports: Use Secure Cloud Identity and Access Management Practices and Managing Risk from Software Defined Networking Controllers.

Best practices

Secure networking practices adhering to ZT principles are vital to ensure the security of cloud resources. Cloud customers should follow these best practices to help prevent, detect, and respond to threats to the cloud environment:

- Connect to the cloud environment and cloud resources through a secure encrypted channel. NSS must use CNSA-approved cipher suites for all client connections. Other organizations should use CNSA or NIST recommended cipher suites.
- If using the cloud for more sensitive workloads, consider using private connectivity options.
- Be aware that data passed between customer resources in the cloud may traverse the Internet, and take precautions to encrypt such data.
- Employ micro segmentation practices, separating traffic between services that do not require communication paths. Configure firewalls within the organization's tenant to separate compute instances from each other, only allowing necessary data flow paths.
- Monitor use of traffic mirroring services for potential malicious exfiltration attempts.

Further guidance

Additional cybersecurity guidance can be found at NSA Cybersecurity Advisories & Guidance. Some papers that build on the topics discussed in this CSI include:

- Hybrid and Multi-Cloud: When moving from a single cloud to a hybrid cloud or multi-cloud environment there are additional complexities introduced. For more details on how to address these complexities, see Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments.
- Logging and Threat Hunting: It is vital for organizations' threat hunting and incident response professionals that network traffic be thoroughly logged. For more details on what to log in cloud environments, see Manage Cloud Logs for Effective Threat Hunting.

- Embracing a Zero Trust Security Model
- Selecting and Hardening Remote Access VPN Solutions
- Network Infrastructure Security Guide
- Configuring IPsec Virtual Private Networks
- Managing Risk from Software Defined Networking Controllers
- Managing Risk from Transport Layer Security Inspection

Additional cybersecurity guidance from CISA includes:

- Trusted Internet Connections 3.0: Cloud Use Case

Works cited

[1] National Security Agency. Announcing the Commercial National Security Algorithm Suite 2.0. 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
[2] National Institute of Standards and Technology. Cryptographic Standards and Guidelines. 2023. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
[3] National Institute of Standards and Technology. FIPS 140-3: Security Requirements for Cryptographic Modules. 2019. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
[4] National Security Agency. Selecting and Hardening Remote Access VPN Solutions. 2021. https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF
[5] National Security Agency. Network Infrastructure Security Guide. 2023. https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF
[6] National Security Agency. Configuring IPsec Virtual Private Networks. 2020. https://media.defense.gov/2021/Sep/16/2002855928/-1/-1/0/CONFIGURING_IPSEC_VIRTUAL_PRIVATE_NETWORKS_2020_07_01_FINAL_RELEASE.PDF
[7] MITRE. Automated Exfiltration: Traffic Duplication. MITRE ATT&CK. 2023. https://attack.mitre.org/techniques/T1020/001/
[8] National Security Agency. Managing Risk from Transport Layer Security Inspection. 2019. https://media.defense.gov/2019/Dec/16/2002225460/-1/-1/0/INFO%20SHEET%20%20MANAGING%20RISK%20FROM%20TRANSPORT%20LAYER%20SECURITY%20INSPECTION.PDF
[9] CISA. Trusted Internet Connections 3.0. 2023. https://www.cisa.gov/sites/default/files/2023-05/tic_3.0_cloud_use_case_508c.pdf
[10] National Institute of Standards and Technology. Glossary. 2019. https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

Disclaimer of endorsement

Trademarks

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk:
NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov
CISA Media Inquiries: 703-235-2010, CISAMedia@cisa.dhs.gov