tufin The Security Policy Company.

A Strategy Guide to Network Segmentation Best Practices & Methods

About this Guide

This guide is for organizations that wish to develop and execute an effective network segmentation strategy. It explains the strategic goals for risk, compliance, and security, and how to achieve these goals. This guide also includes common challenges and avoidable pitfalls to make your network segmentation project successful.

About Network Segmentation

Segmentation is the division of an organization's network into smaller and, consequently, more manageable grouping of interfaces - segments a.k.a. zones. These zones consist of IP ranges, subnets, or security groups designed typically to improve performance and security. In the event of a cyberattack, effective network segmentation will confine the attack to a specific network zone and contain its impact by blocking lateral movement across the network via logical isolation through access controls.

PCI-DSS (Payment Card Industry-Data Security Standard) and other security standards provide guidance on establishing clear separation of data within the network. For example, organizations required to satisfy PCI-DSS standards must separate the network for Payment Card authorizations from the Point-of-Sale. Organizations that need to comply with NERC CIP (North American Electric Reliability Corporation) must ensure that critical assets do not connect directly to the internet. With a sound security policy, organizations can segment the network into multiple zones that reflect the configuration of their security access controls and provide a referenceable model for determining if future access changes are permissible from a zone-to-zone perspective.

When conceiving of a network segmentation strategy, it is also important to avoid oversegmenting as this may result in a loss of manageability and scope. Although segmentation is often viewed as a solution for significant challenges in compliance, security, and connectivity, organizations must move incrementally to assess the current state of manageability and avoid overcomplicating the network. Provided their segmentation approach remains manageable, organizations will undertake a more granular approach called micro-segmentation which pursues a state of **Zero Trust**.

Segmentation Benefits

IT Governance and Risk Management

Segmentation operationalizes security policy into a referenceable benchmark that delivers visibility into existing compliance violations and enables proactive identification of access requests that violate compliance. Effective risk identification and mitigation (or exception tracking) enables organizations to achieve policy health, comprehend their state of assumed risk, and drive future changes with IT governance built into the change management process.

Compliance

Segmentation consists of access policies that specify which services are allowed or blocked between network segments. By modeling these security policies, compliance can be established. Establishing this baseline of acceptable access through permitted services enables organizations to identify and clean up inherited violations and preclude the introduction of new ones. Business requirements may conflict with stated security policy from time to time. The resulting violations should be designated as exceptions and tracked for recertification to avoid non-compliance. Recertification processes ensure necessary connectivity and eliminates the inadvertent failure of an audit by not accounting for exception-based, non-compliant access. Solutions are available that can automate the recertification, rule changes and documentation, and allow organizations to maintain a consistent audit trail of rule certifications.

Establishing a referenceable access policy between network segments also provides a consistent baseline that can guide future decision-making. Rather than relying on an internal knowledge resource, network engineering (or security) can quickly assess the compliance of access requests assigned to them. Compliant access requests are designed, configured, and noted as compliant for audit; non-compliant access requests are typically rejected with an option to submit the access request as an exception with an expiration. If approval over a non-compliant rule is provided, the exception rules within the environment are known, well documented, and consistently reviewed for recertification.

Through this policy reference documentation and compliance modeling exercise, your organization will come to a consensus on what constitutes "risk". Consider sensitive data or critical assets in a network zone. This zone requires connectivity to another zone, but you will still need to be aware of what services are considered secure between two zones, or those that may be less secure and more vulnerable (e.g. TCP through port 22). Even if your segmentation model allows TCP, you still must monitor the rule for usage (as a spike may indicate a compromise) and, if unused, remove it from your available policy.

Security

Designating zones allows organizations to consistently track the location of sensitive data and assess the relevance of an access request based on the nature of that data. Designating where sensitive data reside permits network and security operations to assign resources for more aggressive patch management and proactive system hardening.

Beyond designating zones for greater scrutiny over access, segmentation provides a logical way to isolate an active attack before it spreads across the network. The designation of zones and allowable services between them provides a manageable way to identify and mitigate vulnerable access paths being exploited during an attack.

Preparing to Segment

Get Started

Organizations commonly undertake a segmentation strategy without establishing an actionable starting point. IT security is typically familiar with the network locations where business units or teams reside, which are often designated as zones. However, assigning a zone to each of these business entities in a large organization often creates too much complexity to start with.

Organizations seeking a starting point typically find that designating rudimentary network zones is the most successful approach. Simple zones used to begin segmentation include Internal, External, Internet, and DMZ. Starting with these zones, refinements to access policies are easier to make, ultimately resulting in an acceptable policy.

Develop a Baseline

Organizations need to start small by agreeing to a standard policy for allowable services between zones. And if your company's security policy is stored in the mind of "The Compliance Guy," it is time to transition from the spoken tradition of policy documentation and transcribe the knowledge to Excel or Word. In addition to ensuring that security policy will not be amended due to a memory lapse or unexpected sick day, documenting security policy establishes a minimal referenceable benchmark for compliance. Once security policy is transcribed and centralized in a single place, each decision to modify access policies is made consistently and confidently.

In cases where "The Compliance Guy" lacks a strong grasp of what constitutes allowable services between zones, IT security professionals are best advised to collaborate with peers or consult technical leadership to develop a security policy model. If you are the lone in-house IT security professional, you should reach out to any established vendors in the space that can provide guidance on developing a security policy. Your existing vendors have likely provided similar guidance to customers and may have repeatable best practices that they can share with you.

Identify Ownership

Different vendors are selected for different networking devices and platforms, and those platforms are increasingly managed by different business units with different priorities (e.g., DevOps controlling public cloud). As you prepare to define and enforce network segmentation across your hybrid network, now is an ideal time to determine which of the different parts of the network fall under your purview and ownership. In the event of a security incident, each team will have responsibility to contain a breach, but only by establishing ownership over the network will you know the exact scope of your own personal accountability and response requirements. Often, this inquiry aligns two teams around a unified goal and provides an opportunity to improve the network's connectivity and security to everyone's benefit.

Identifying ownership should also include any upcoming new networks. When you identify parts of the network you are responsible for segmenting, you will also want to include any anticipated networks that may be adopted or merged with your existing network. By understanding that these changes will impact your network segmentation strategy by introducing new security concerns and imposing obstacles in ensuring connectivity, you can account for them in timeline planning.

Ensure Manageability

Parallel to ongoing changes in networking platforms are changes to network policy. Your organization may undertake a cloud-first initiative, launch new businesses, or open new locations across the globe. Regardless of what changes in your network, there needs to be consistency over managing and tracking these changes.

Often, organizations already have existing tools used by a person on another team or even a product previously purchased for another purpose that aligns to your current segmentation goals. Identifying tools that have previously been configured on your network or are currently used to manage your network makes managing your segmentation process achievable from the start. And if you do identify multiple existing solutions, consider whether you can integrate them to develop a more enterprise-ready solution that can be used as a central console for designing, implementing, and managing ongoing segmentation controls.

In a scenario where there are no existing tools in use, query internal resources to determine who has experience in segmentation, regardless of how basic, and use that as a starting point to assess tools. An often-overlooked solution is to consult with any of your network solution vendors to determine if they have solutions and guidance on using their tools to manage network segmentation. Often, a solid relationship with your account manager can extend support beyond product purchasing requirements.

Develop a Phased Plan

By this point in the process, you know which resources are available to you, the personnel who can contribute to segmentation design and implementation, and the external guidance you can utilize to technically execute segmentation. Armed with this knowledge, you can assess priorities.

First and foremost, assess the network from the high level and consider what zones you will want to appoint regardless of how rudimentary it seems. Even segmenting the network in half will provide you with greater management over connectivity, increase visibility over access, and identify risks associated with existing access rules. Taking the first rudimentary step to designate four zones—Internal, External, Internet, and DMZ—also enables you to start identifying connectivity restrictions if they are not known and to prioritize which of the zones should be further segmented (e.g., sensitive data, cyber assets).

If you are required to comply with a regulatory mandate, start by designating a sensitive data zone (like for example a zone for PCI-DSS systems and data). Should you start on this granular level, you can begin with compliance in mind and then take a step back to approach the broader network.

In any event, you will want to further segment these initial zones (e.g. Internal can be segmented by function). This approach develops a greater understanding of connectivity improvements, prioritizes access reduction, and reduces the likelihood of a successful attack to access sensitive data. As your segmentation initiative continues, take the opportunity to realize a greater degree of granularity. SDN solutions, such as VMWare NSX-T or Cisco ACI, provide flexible methods to develop individual access control for applications in a security-first mentality referred to as microsegmentation. However, applying such defined security controls must be undertaken gradually, as implementing such detailed control in security groups can become unmanageable due to the sheer volume of individual security groups.

Segmentation Pitfalls

Undertaking Too Much

Organizations often undertake segmentation to increase control over the network, but establishing security controls with too much granularity produces over-segmentation. Often, organizations will try to undertake too much at once or define a lofty goal of nanosegmentation—the practice of the most granular level of access control—at the outset. This results in "analysis paralysis" during ongoing management of access control changes. If a security group is assigned for every application in a 500-application environment, in addition to traditional segments, there are an additional 500 segments. And rather than reuse a zone, it is simpler to create a new security group for application access. The sheer volume of zones produced by this method will overwhelm a team and leave organizations in a state of overcomplication without an ability to prioritize security between zones.

Another often-encountered outcome of over-segmentation is overly complex policies. Because of the high degree of control over policy for each zone, organizations may over-architect policy of a zone to fit very specific access requirements. This degree of granularity meets initial policy requirements, but quickly becomes overwhelming when security analysts need to analyze policy without context and design future changes.

Segmentation can help secure and enable the business, but it should not be undertaken to a point where it impedes agility goals.

Failing to Act on Information

In the security world, automated solutions send an overwhelming amount of alerts. When the amount of populated data surpasses the ability to process, prioritize, and utilize them for decision making, your invested time and resources fail to produce results. In this scenario, your decision-making processes break down and tools you have built or bought become shelfware.

Provided that you have been able to configure alert mechanisms for policy violations, it is important to delineate these from other triggered alerts to address them in a consistent and effective method. Violations to security policy should be promptly reviewed to determine if they should be designated as exceptions, and tracked for recertification to retain compliance. Beyond a compliance measurement, it is important to assess whether access violations are intentional and are approved through the proper review process. Given that security professionals are often ideal targets of APTs, flagging violations for review is not only important for compliance, it is crucial to ensure that an attacker has not compromised credentials and is granting themselves access to further their attack into network zones containing sensitive data.

Halting Segmentation

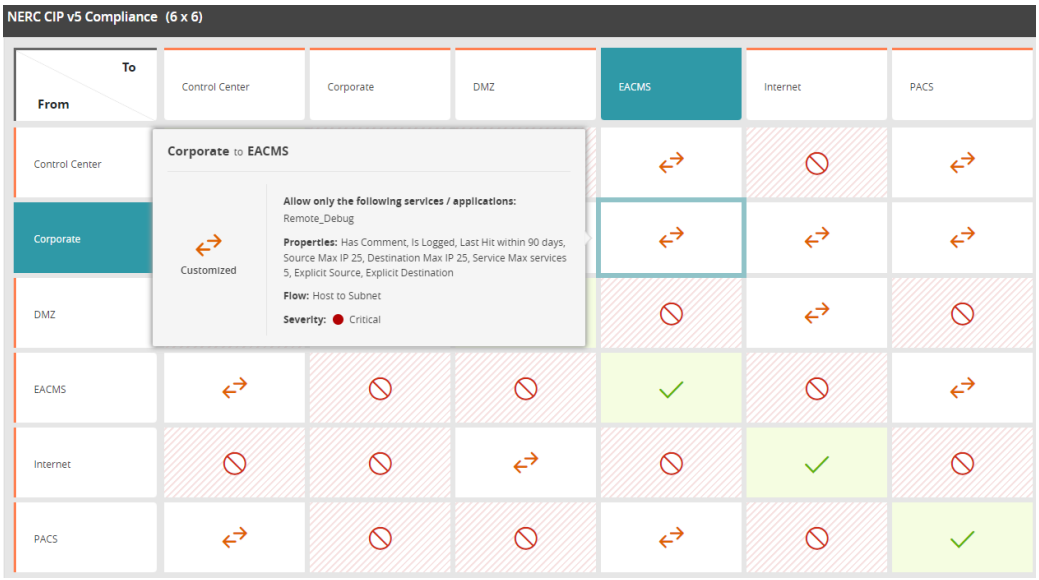
Segmentation needs to be approached as an incremental process without a defined state of completeness. The network is subject to change and so are the access controls governing connectivity. Knowing that "security is a journey, not a destination," a continuous approach is best. Breaking segmentation into manageable steps in a phase-based approach will enable competing initiatives to be undertaken in parallel without impeding segmentation. A step forward provides you with the opportunity to review, revise, and continue the momentum.

Has your company acquired other businesses that require network connectivity? Organizations will often leverage a basic or best practices security policy and apply a rudimentary segmentation model within acquired networks to understand the current state of risk and prioritize mitigation efforts. Organizations can then manage the acquired networks in their own segmentation model, or merge network zones to existing zones if comfortable with the state of known risk.

Other compelling points for retaining an ongoing segmentation strategy is utilizing multiple platforms such as cloud or a future purchase of a solution that improves network segmentation manageability.

The Tufin Solution

Tufin offers a zone-to-zone connectivity matrix called the Unified Security Policy (USP) that enables the definition or selection from templates determining which network zones could connect when asked, and the access allowed or blocked between the two.
The USP enables Tufin SecureTrack users to develop a visualization of their network access policy across all vendors and devices and define the services permitted. Existing access policies that violate the compliance model are flagged, and may also be designated as an exception and tracked for recertification, while unnecessary policies are removed through automated workflows. The Unified Security Policy integrates into change management workflows to bake compliance into every change and reduce the obligations of network security teams to review every access request. When used with the Tufin Rule Lifecycle Management extension, organizations can configure and orchestrate rule review processes to ensure consistent compliant processes are adhered to for managing risky access.



Tufin's Unified Security Policy Matrix for NERC CIP Risky Services

The Security Policy Builder app further enables security teams to easily analyze access between segments throughout the network (cloud and on-premises), to create a visual model, and – most importantly – recommend a comprehensive access-based security policy based on the analysis of existing access in addition to available compliance-based models (e.g. PCI-DSS, NERC). All historical decisions regarding access are based on the risk framework of network segmentation, while all network access change implementations can be implemented, verified, and tracked through Tufin SecureChange.

Tufin allows security teams to confidently build a segmentation strategy with the visibility and automation to effectively secure policies across hybrid environments and ensure network access change requests take minutes and not days.

Learn more at tufin.com/solutions/network-segmentation

About Tufin

Tufin provides a single platform for network and cloud security teams to simplify the management of security policies across today's complex, multi-vendor hybrid networks. The platform gives some of the largest companies in the world the end-to-end visibility and automation tools necessary to swiftly provide new access, enable fast and secure application deployment, and ensure continuous compliance and audit readiness.
Tufin's proven solutions help more than 2,000 customers across industries including healthcare, financial services, utilities, telecommunications and retail to quickly identify and mitigate network risks. For more information, please visit www.tufin.com.

DP20220222