White Paper

FORESCOUT

Dynamic Network Segmentation

A Must-Have for Digital Businesses in the Age of Zero Trust

Table of Contents

01 INTRODUCTION: Digital Transformation Mandates a Network Security Rethink

01 SECTION I: Point Solutions Fail to Address the Issue

03 SECTION II: Dynamic Network Segmentation Defined

04 SECTION III: Dynamic Network Segmentation Defined in Action

05 SECTION IV: Business Benefits of Dynamic Network Segmentation

06 SECTION V: Conclusion and Guidance

INTRODUCTION: Digital Transformation Mandates a Network Security Rethink

The IT landscape is rapidly evolving to meet the demands of our digitally transforming world and a radically changed business environment that calls for always-on performance and agility at scale. As a result, client-server computing has given way to disruptive IT architectures that reshape business and ownership models. These include private and public cloud services, ‘bring your own device’ (BYOD), mobility and the Internet of Things (IoT). This shift has given rise to new, innovative market leaders and provided additional opportunities for existing businesses and their stakeholders.

Yet, digital transformation has also created unique security challenges which traditional solutions were never designed to address. Foremost among these challenges is the erosion of the corporate network perimeter. As users, devices and apps constantly interact within and beyond corporate firewalls, IT can no longer secure a defined network perimeter. The situation will only intensify with the continuous proliferation of IoT devices. According to IDC, the number of IoT devices will increase dramatically over the next several years and reach 55.7 billion by 2025.[1]

As executive teams call for more operational and business agility, IT leaders must apply a modern, unified security solution that dynamically segments the new corporate network to secure users, devices, workloads and apps – regardless of their location. Doing so is a critical step toward the adoption of a true Zero Trust security posture.

SECTION I: Point Solutions Fail to Address the Issue

Traditional security architectures, and most modern point solutions for security, still reflect thinking from the client-server era, when just a single ingress point from the outside existed and the IT department owned and controlled all applications, infrastructure and endpoints. Such architectures have rigid designs. As IT teams adopted ‘flat networks’ for improved uptime, access and speed, point security solutions were introduced to address specific threats. Unfortunately, organizations continue to have an incomplete picture

[1] 27 Jul 2020, *IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC*. Downloaded June 30, 2021, from the following source: IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC

of the threats appearing on their networks. This results in the five major challenges which IT leaders must overcome:

Challenge #1: Increased threat complexity: Persistent threats (attacks that circumvent existing defenses, go undetected and cause continuous damage) are difficult to detect. The first step to combat such advanced threats requires an organization to obtain up-to-date information about all of the physical and virtual endpoints across the network, including laptops, PCs, smartphones, tablets, BYOD and IoT endpoints, servers, virtual machines, cloud instances and more. IT must gain granular information about each: its function, how it is connecting, its security posture and the list of apps and devices that interact with it. Only after gaining these insights can IT develop a 'defense-in-depth' security approach – one that involves diligent separation of assets based on their function in order to minimize the lateral spread of malware across the network. Traditional security products operate in silos, making it unrealistic to proactively identify all physical and virtual assets, separate them based on their business function and stop the lateral movement of threats between them.

Challenge #2: New security threats created by IoT: The IoT era is here, and the headless devices that come with it have no inherent security capabilities. If they are breached and are not compartmentalized within their sphere, they can create back doors into a company's network. Shadow IoT/OT is becoming a particular concern for network and security teams. Lack of oversight often results in users adding new IoT or OT devices to networks without the IT team's knowledge. The following are a few commonly occurring examples:

- OT teams add their own IoT devices to the network.
- Mobile workers/employees, contractors and other third parties bring in their own devices (i.e., smart watches, speakers, personal tablets, etc.) and connect them to the network.
- Snack and soda machines 'call home' via the corporate network and out to the Internet to provide information regarding temperature and stock levels.

A lack of visibility into these devices, combined with the inability to detect the type of device being used, creates enormous challenges for IT and security teams tasked with monitoring and segmenting these devices.

Challenge #3: Lack of agility: Today, businesses need to move rapidly to take advantage of opportunities in a hyper-fast and efficient competitive landscape, underscoring the need for agile IT. Traditional security relies on deploying best-of-breed point products at specific points in the network. In this model, each security tool must be configured individually, which means changes often take months to implement. Additionally, since digital transformation continues to expand to new areas, businesses are relying on an ever-increasing volume of security point products, adding more complexity while hurting agility. How bad is the point product sprawl? The average enterprise has multiple products attempting to do what a single, unified solution should manage better. According to research from the Ponemon Institute, companies deploy, on average, 47 different cybersecurity solutions and technologies.[2]

Challenge #4: Meeting compliance requirements: Organizations, whether they compete in highly regulated industries like finance (SWIFT, NYDFS), healthcare (HIPAA) or less regulated ones, must comply with multiple governmental or industry-imposed regulations. For example, the PCI-DSS

[2] July 30, 2019. Ponemon Study: 53 Percent of IT Security Leaders Don't Know if Cybersecurity Tools are Working Despite an Average of $18.4 Million Annual Spend. Downloaded June 30, 2021, from the following source: Ponemon Study: 53 Percent of IT Security Leaders Don't Know if Cybersecurity Tools are Working Despite an Average of $18.4 Million Annual Spend | Business Wire

standard applies across any industry in which merchants or providers receive payment by credit card.

PCI-DSS provides guidance on creating clear separation of data within the network such as separating the network for Payment Card authorizations from the network for Wi-Fi traffic. A sound security policy entails segmenting the network into multiple zones, with varying security requirements, and rigorously enforcing the policy on what is allowed to move from zone to zone. With numerous standards and regulations calling for similar measures around network and data security, the challenge grows as the volume of external threats originating from the perimeter and within internal networks grows.

Challenge #5: Complexity of securing the data center: Software-defined data centers have enabled organizations to do much more within the same amount of space, with greater flexibility, speed and cost efficiency. Yet, they also create challenges for security teams that are using unfamiliar and siloed security tools. The situation allows attackers to take advantage of noncompliant and vulnerable endpoints. With the majority of traffic within data centers moving in an East-West direction, security leaders need a new approach to protect such environments and ensure that they are compliant with company security policies.

As these five challenges demonstrate, businesses need to complement security investments made at the perimeter with technologies that can protect the internal network. Traditional perimeter security alone is not sufficient in a world where everything is connected and more threats are coming from inside the network. Security success certainly requires protecting the perimeter. Yet, IT cannot rely solely on perimeter protection, just as a castle that was once protected by a moat also needed to employ internal guards.

These changes and challenges have reinforced the need to build networks based on least-privilege access, also commonly referred to as 'Zero Trust.' This is why industry leaders are shifting budgets away from perimeter-only spending and adopting solutions that protect the internal network. While they must maintain perimeter security, they recognize that the majority of attacks target areas inside the perimeter. The natural security posture that results is one that provides ***dynamic*** network segmentation in a manner that grants least-privilege access for all security initiatives.

SECTION II: Dynamic Network Segmentation Defined

Dynamic network segmentation represents the logical next generation of segmentation. Traditional network segmentation leverages virtual local-area networks (VLANs) and access control lists (ACLs) to logically separate the network into secure zones, with each zone compartmentalized and isolated from the other segments.

Dynamic network segmentation works on the guiding principle that security must be ubiquitous and transparent to the network, allowing organizations to segment their network in an effective and meaningful manner across the campus, data center, cloud and OT. It involves discovery and precise classification of users as well as all types of network-connected physical and virtual endpoints, their security postures, levels of compliance and additional, relevant security information.

Dynamic network segmentation operates on an approved (white list) model, whereby no device or user can see any other unless the list created by IT explicitly enables it to do so. Once the white list is established, endpoints are confined to their groups. For example, IT can set up a security policy that states, “medical devices can connect only to the medical records server” or “a security camera (which can be an IoT device) can connect only to the video server.”

This approach dynamically prevents devices in a guest network from having access to these endpoints and limits access to their functions without connecting to the outside Internet. As a result, any unauthorized user cannot gain access to devices located in the network’s other zones. If, for example, a medical device moves within the network, the policy follows that endpoint device, eliminating the need to reprogram the network. Similarly, in the retail industry, IT can create separate, secure zones for the point-of-sale (POS) equipment, guest network and accounting department. This would ensure that people connected to the guest network cannot access separate segments that IT designates as specific only to POS devices.

Through intelligent orchestration and automation of security policies, dynamic network segmentation dramatically reduces the manual effort involved when changes occur in the network and provides security for heterogeneous networks. This gives IT leaders the freedom to use diverse network infrastructure. The explosion of attached devices is being fueled by the IoT and OT device proliferation.

Dynamic network segmentation grows in importance proportionally to the growth in connected device volumes. With billions of devices already connected to networks, organizations are quickly realizing the critical role that dynamic segmentation already plays in ensuring that IT can limit the blast radius of any breach.

SECTION III: Dynamic Network Segmentation Defined in Action

Next-generation firewalls (NGFWs) deliver network segmentation by ensuring appropriate application and user access, along with inspection for all traffic crossing the segments. However, only a portion of internal network traffic flows through NGFWs. For example, internal traffic not headed for the Internet or within specific network domains (e.g., operational technology) may not pass through the firewall, and therefore, goes uninspected. When organizations realize that relying on NGFWs for Zero Trust requires them to add new security tools and re-architect their entire network, they grow wary of the potential costs and cancel most projects.

Dynamic network segmentation provides a more cost-effective alternative, because it leverages existing infrastructure and helps organizations start a Zero Trust journey without breaking the bank or requiring a complete redesign of the existing network.

Instead of re-architecting one’s network, dynamic network segmentation provided by the Forescout platform integrates with the existing network infrastructure across the campus, data center, cloud and OT to discover, profile and classify traditional and non-traditional devices (laptops, PCs, tablets, smartphones, BYOD and IoT endpoints, servers, virtual machines and cloud instances). It then assigns these entities to groups/roles – without the need for agents. This enables IT organizations to implement dynamic segmentation using granular access policies based on user identity and device context, regardless of device or user location on the network. In turn, secure access to critical services is ensured, preventing unauthorized access to sensitive resources and helping to minimize data breaches. Additionally, this improved visibility makes it easy for a business to obtain true counts and identification of its existing asset inventory tools, such as configuration management databases (CMDBs), with real-time information about network-connected devices, users and the associated security contexts.

SECTION IV: Business Benefits of Dynamic Network Segmentation

Dynamic network segmentation delivers the agile security posture which businesses need to pursue their digital transformation strategies. As a critical enabler of digital strategies and Zero Trust initiatives, dynamic network segmentation delivers the following benefits:

Boosts IT's role as a business enabler: Because dynamic network segmentation does not require a complete redesign of the network, the business is free to pursue new operational models and know that security concerns will not slow their progress. In fact, Forescout's dynamic network segmentation capabilities provide pre-implementation simulation features that simulate the impacts of new and revised policies. IT teams no longer worry about disrupting business processes as they secure whatever new operational model they choose.

Simplified security architecture: Security has evolved, with new point products being developed to solve specific problems. All of these new technologies have created security sprawl, where security professionals need to continually configure and update a wide variety of network and security infrastructure every time a change is made. Additionally, these technologies create their own silos, adding to management complexity. Because dynamic network segmentation provides access regardless of user location or device location on the network, it acts as an enabler for IT and security teams by greatly reducing their administrative tasks.

Improved productivity of IT staff: A major challenge of managing traditional security technologies involves the need to constantly add, change and delete rules. Often, IT administrators will ignore the step of deleting old rules to speed their progress and avoid tedious tasks. Yet, when old and new security policies exist, conflicts between them can lead to confusion and even breaches. Dynamic network segmentation can greatly reduce the needless IT overhead associated with having to manually identify, classify and onboard traditional and IoT devices and include them in policies for network access.

Superior access without compromise: Businesses can create unified policies that automatically adapt to changes, such as the addition or movement of servers or devices, without manually modifying each rule. When a new device connects to the network, it is automatically categorized and grouped based on its function, device type, location and additional factors. In the end, employees and users gain unhindered network access without posing a security risk.

Improved regulatory compliance: Segmentation can help businesses operating in regulated industries meet regulatory demands and standards.

In healthcare, for example, IT can apply dynamic network segmentation to establish zones for medical devices and servers. In this case, patient records are stored in their respective compartments in order to secure patient information, records of procedures and doctors' notations while restricting the access of medical devices within their zones – making them unreachable from any other network or device.

SECTION V: Conclusion and Guidance

In today's fast-moving digital business environment, it's imperative that organizations rethink their security strategies and implement a solution that can bring the same level of agility to security that other areas of IT have today. Security must act as an enabler and support organizations' digital transformations.

Dynamic network segmentation solutions, such as Forescout, complement existing infrastructure and maximize a company's investments, making it a critical and high-ROI business enabler. From a security standpoint, dynamic network segmentation needs to be a top initiative for all organizations. As you consider your own dynamic network segmentation initiative, follow the guidance below to help develop strong Zero Trust-based segmentation.

Know what you want to segment. While many organizations want to extend segmentation beyond microsegmentation within the data center, not knowing where to begin dooms many projects at the outset. Starting with one or two use cases will help demonstrate early success and accelerate adoption. Once you have solved for those targeted use cases, begin to expand your program.

Gain 100% device visibility. Even though you're starting small, it is impossible to build an effective security strategy without having a good understanding of network-connected physical and virtual endpoints, users, applications and services. The process of securing the network must begin with gaining complete visibility of all network-connected devices, managed and unmanaged, and taking inventory of them. This baseline of data will provide the information you need to make informed business decisions.

Baseline existing data flows/communication patterns. Before you begin with segmentation, you need to know where you are starting by understanding existing data flows and communication patterns so that you recognize and identify legitimate and anomalous traffic patterns.

Build out your segmentation policies and implement dynamic network segmentation. Automation to logically group assets based on user, device type, business function and more allows for quicker and more accurate policy creation and management. This establishes how your network will dynamically adapt to changes or the movement of resources.

Maintain continuous compliance. Once you have real-time and agentless visibility into the network, you can orchestrate, automate and enforce compliance at the moment of device connection, with remediation actions prescribed beforehand. A technology like Forescout's provides continuous monitoring and alerts you when a device or user violates a policy. The monitoring extends to real-time threat detection, an especially important aspect to protecting IoT and OT networks. If initial segmentation does not address all potential threats, Forescout's monitoring and alerts enable you to detect this and respond via increased segmentation or ad-hoc control actions.

Start with a targeted use case

Know what is on your network

Baseline existing traffic

Automate policy creation

Monitor and enforce compliance

Learn more at Forescout.com

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591