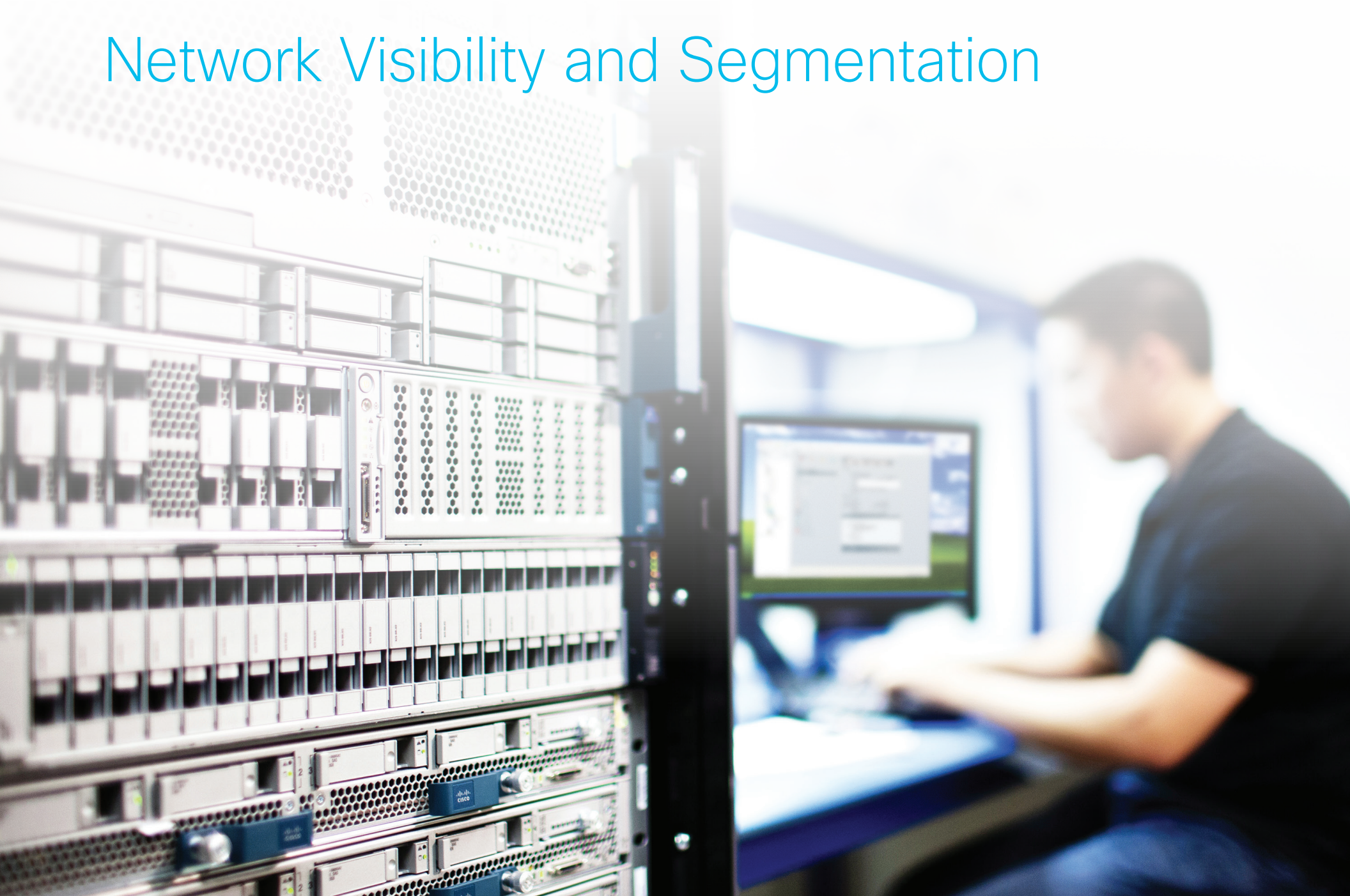
Network Visibility and Segmentation



Contents

Network Segmentation – A Services Approach

Many organizations today are considering network segmentation as a strategy to improve their overall security posture. Network segmentation is intended to reduce the ability of threat actors to move freely throughout the enterprise once an initial breach has occurred.

A segmented network creates secure boundaries around sets of critical assets using controls to restrict access and gain visibility into traffic flows and user behavior. While segmentation is generally recognized as a security best practice, practical implementation can be challenging to scale and manage in today's dynamic environments. Without proper planning and preparation, segmentation projects can prove overwhelming even to the most advanced and mature IT organizations.

This document describes Cisco's framework for a complete end-to-end solution for network segmentation delivery. It defines six components that must be considered for a successful implementation. It also describes a services approach for planning, implementation, and ongoing operation.

The Process of Segmentation

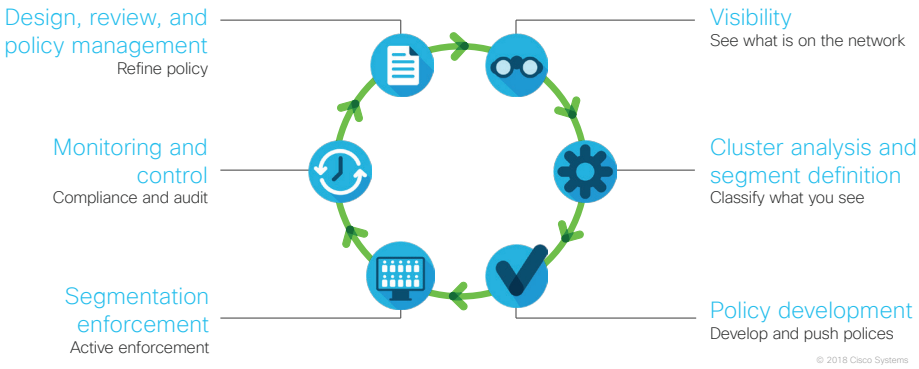
Enterprise network segmentation is a very complex undertaking. The most successful segmentation projects begin with planning and design efforts to establish a segmentation strategy that meet the requirements specific to your organization. No single product solves the segmentation problem; rather, effective strategies adopt a process approach to segmentation.

This process requires setting the proper goals, gaining visibility into actual network traffic, identification and classification of the assets that are to be segmented, building policy to enforce the segmentation, propagating policy, and then maintaining the policy. Further, due to the dynamic nature of today's networks, a continuous operational process is required to understand network changes and decide if new policy needs to be distributed. Essentially, this means that as part of your planning and process definition, you will also need to look at defining how you operationalize your segmented environment.

Segmentation should be viewed as a continuous journey that, if approached properly, results in effective protection for critical assets and a much more secure network.

Segmentation Solution Components

There are six components to a segmentation solution as visualized in the graphic, and further defined in the section below.



Design, Review, and Policy Management

It is critical to align business outcomes to your segmentation strategy. This begins by defining the segmentation goals for the enterprise. What are the business drivers behind the segmentation initiative? What assets are you trying to protect? What threats are you most concerned with? What technologies are deployed? What does your technology roadmap look like? What are your priorities? What are your pain points?

This information helps define the high-level strategy by gaining an understanding of business goals and drivers, critical business assets, known risks and an overall understanding of the current enterprise security posture. This in turn helps us determine next steps and priorities for reducing security risk and developing technology roadmaps

The outcome of this effort allows us to document a high-level segmentation strategy around identification and classification of assets, technology utilization, trust strategies and implementation roadmap and priorities. The end result of performing this function is to have a plan, and to set proper expectations around what you are trying to accomplish through segmentation in the first place. What is the journey going to look like, and how will you know when you are finished? Answering these questions is critical for understanding how you will accomplish your objectives, and how you will drive your segmentation program through short-term wins tied to an overall strategy that can that can be measured for success along the way.

Visibility

Traffic visibility and device identity are crucial components of a segmentation project. With the high-level segmentation strategy and priorities defined, a plan can be developed for data collection to support the projects' visibility requirements.

This plan has a few primary considerations: 1) types of traffic of interest (North, South or East, West); 2) types of devices collecting traffic (physical or virtual): 3) location for best sources of data (WAN edge, Access Layer); 4) best sources of data (NetFlow, SPAN); and, 5) the appropriate analytics platform (Stealthwatch and/or Tetration).

The output from this process identifies devices within a segment, identifies trusts (policy) with other segments, and can be very useful in the discovery of unknown devices and traffic patterns.

The visibility exercise provides data validation to support and augment the discovery completed with defining the segmentation strategy. This stage is crucial in understanding if, how, and where you might need to make adjustments to your strategy based on the actual happenings in your environment.

Cluster Analysis and Segmentation Definition

Leveraging the traffic visibility efforts, each end-point must be classified and associated with a segment. For instance, if a hospital sees radiology gear as a critical asset, then those devices should be identified and grouped with like devices. This is usually accomplished through traffic pattern analysis and through the integration of external system data such as Active Directory or Configuration Management Database (CMDB) which allows us to group systems and end-points that can be the appropriate segments.

Most organizations may not have sufficient visibility or CMDB/asset tracking, making these early phases in the segmentation process crucial to help organizations bridge the known and unknown gap in their existing environment.

Segmentation Policy Development

At this stage enforcement policies are developed—with segments defined, end-points discovered and documented, and trust relationships understood.

The segmentation technologies will determine the specific policy format and enforcement mechanism. These policies can then be reviewed by stakeholders and verified for function before final distribution.

Segmentation Enforcement

Segmentation policy enforcement is a critical milestone in a successful segmentation strategy. Segmentation policy enforcement requires the identification of end-points either by IP address, end-point/user authentication, device profiling or some other method so that polices can be enforced.

Segmentation policy enforcement uses technical controls such as a combination of traditional methods like VLANs/ACLs and firewalls, along with software defined segmentation such as Cisco TrustSec, SD-Access, Cisco Application Centric Infrastructure (ACI), or other enforcement technologies.

Policy enforcement is a key milestone in segmentation, but never the last step in the process.

Segmentation Monitoring and Control

Enterprise systems are very dynamic. Routine changes to the network can quickly create gaps in the segmentation policy that can leave enterprises vulnerable to new threats. Changes need to be monitored daily and policy changes distributed as required. To be effective, segmentation is an ongoing and evolutionary process.

The final step in a successful segmentation deployment requires a disciplined monitoring and control process for continuous audit and compliance. For many organizations, having the tools to prove regulatory/industry compliance is essential for successful risk management. In addition, auditing enforcement policy ensures that the segmentation solution successfully operates as designed.

Cisco Security Services for Network Visibility and Segmentation

For most organizations, segmentation demands a large time and resource commitment. This can be a challenge that indefinitely delays an organization's segmentation and security efforts. Recognizing this, Cisco has developed a services approach to help organizations successfully achieve their segmentation goals.

Security Segmentation Advisory Services

1. Define Objectives

Setting the proper business objectives is critical for the success of a segmentation project. Cisco's Security Advisory team is a group of highly experienced consultants with years of experience helping clients build security architectures that meet their business needs and achieve their security goals.

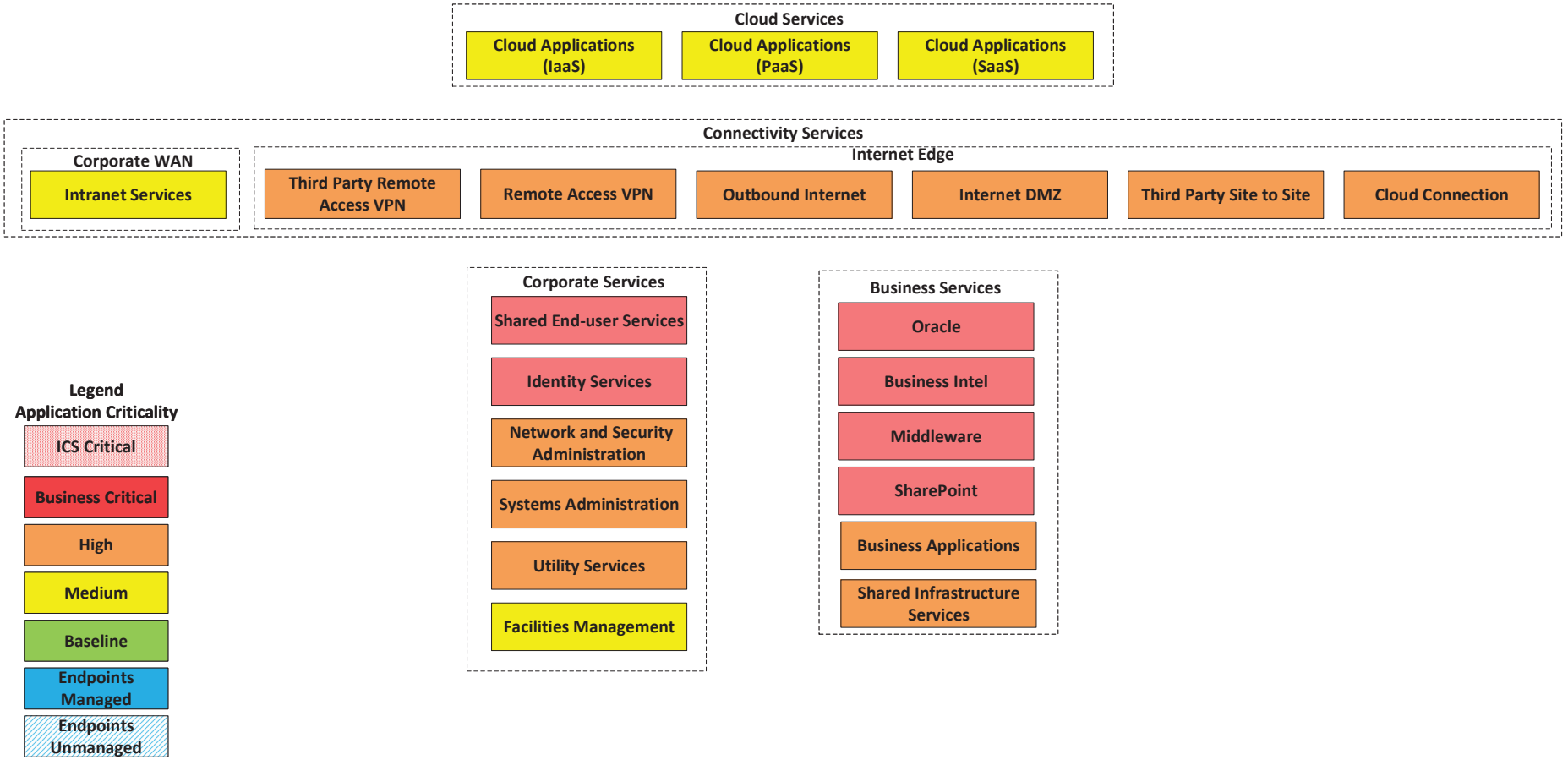
The Security Advisory Services team will help drive answers to common questions:

- What are the business drivers for segmentation?
- What assets are you trying to protect?
- What are the known risks?
- How are assets classified?
- What are the current controls capabilities?
- What is the scope of your segmentation efforts?
- What technology is in place to support segmentation?

The end goal in engaging the Security Advisory Services team is to help you understand the what, where, when and why of segmenting your environment. Setting objectives and laying out a clear roadmap has proven to be the best path to a successful segmentation journey.

2. Identify, Classify, and Prioritize Assets

The Security Advisory Services team then works closely with client stakeholders to define sets of assets that can be readily identified into repeatable design patterns. These design patterns are then classified by business impact, risk, function and/or regulatory requirements. This classification is used to define differentiated security control capability and to help set priorities through clearly defined criteria.



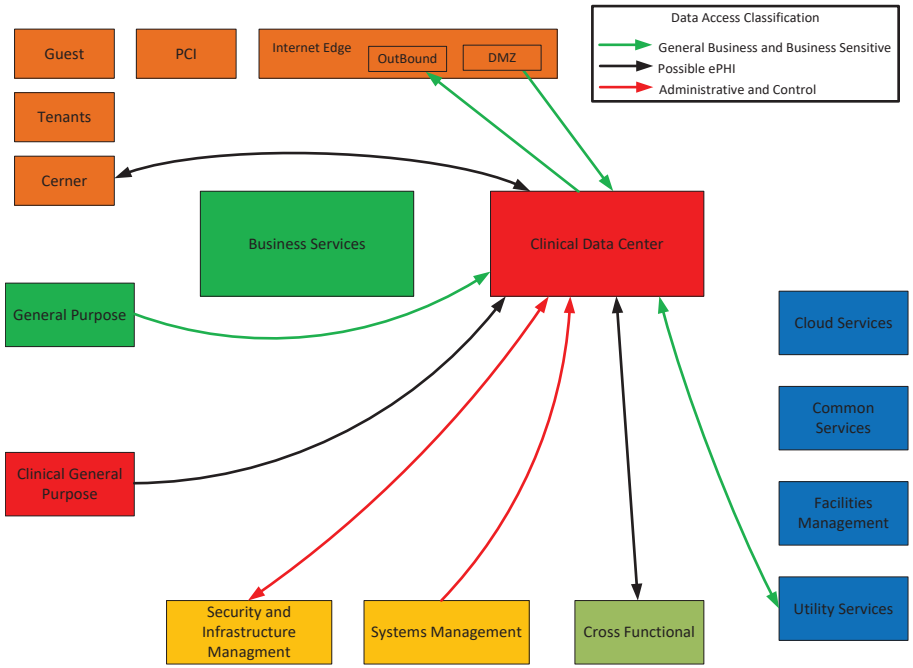
3. Visibility

With the business objectives defined and the asset identification and classification criteria understood we can then use our analysis tools to gain the necessary visibility to validate segment trusts and proper asset identification.

Both Cisco Tetration and Cisco Stealthwatch can be used for this purpose. If the segmentation requirement is for data center only, then Tetration can be deployed. If campus visibility is required, Stealthwatch is leveraged. Both technologies display traffic activity on the network and provide augmented data by which our collective teams can validate or adjust (as needed) any overarching asset identification and grouping decisions that have been made.

Each analytics tool has added segmentation support to perform cluster analysis, which shows us the activity around suggested segments. Based on the output from either of these tools, the Cisco Security Advisory Services team along with the client are better equipped to make enterprise network segmentation decisions for enforcement.

An example diagram of initial cluster analysis is shown below.



By illustrating end-point server relationships and traffic between clusters of like devices, a segment design can be validated and developed to match the client's need.

Security Segmentation Implementation Service

With the business objectives defined and a segmentation plan in place, the Cisco Security Implementation Services team begins the next phase.

4. Detailed Design

Once the segmentation strategy has been defined and aligned with the core business strategy, corporate assets have been identified, grouped and classified and trusts relationships understood, technology specific High-Level Designs (HLD) can be created. The High-Level Design(s) is driven by the client's priority, technology capability and operational impact. Each HLD is then supported by a product specific Low-Level Design (LLD).

The LLD is the specific set of equipment, designs, and configurations that are required for a functioning segmentation deployment. Typically, LLDs include detailed information about the router/switch infrastructure, the network architecture, IP address ranges/subnets, policy enforcement devices such as firewalls, Cisco Identity Services Engine (ISE), and switches with dynamic access control lists, information about logical structures of the network such as proxies, VLANs, and other segmentation technologies.

These components are incorporated into the LLD and used as a deployment "blueprint" for Cisco engineers to create the segmentation solution.

5. Segmentation Policies

The key to a good segmentation solution is functioning, well thought-out segmentation policies. This is where alignment with business objectives is critical. A good segmentation strategy balances simplicity with granularity, placing devices in segments by functional characteristics that are commonly understood, not likely to fluctuate, and generally make sense for the organization.

For example, defining a segmentation approach for a hospital may start with general groups of systems such as hospital administration, labs, pharmacy, and bio-med. This coarse-grained approach provides security posture improvement while reducing complexity and operational impact and allows for later phases to provide more granular segmentation with less overall business impact. If a corporation has three different brands of security cameras, creating individual segments for each brand makes little sense. Instead, protecting all security cameras as a class of facilities management devices would be more efficient to operate. Placing all security cameras in one segment with other security devices, achieves a reasonable balance between the business objective of protecting these devices and managing complexity by grouping similar devices by function.

During the process of defining segmentation policies, Cisco engineers work with the client to maintain policies that achieve a good balance between the business objectives, security posture improvement and operational impact.

6. Validating Policy and Design

With an LLD and Segmentation policies in place, the final deployment model is then reviewed with the client and validated against the original business objectives. This is the last point in the segmentation process to make major adjustments before deployment begins. Cisco engineers review the LLD and policies with the client to confirm the design meets the both functional and technical business objectives, before the final sign-off.

7. Installation of Enforcement Technology

With a validated design in hand, the next step is to ensure the client has the identified enforcement technology installed. This is a major component of the validated design and Cisco engineers will follow the LLD to install, configure, and test all the enforcement components of the solution.

Cisco Stealthwatch and/or Cisco Tetration are key components in a segmentation strategy because they can provide enterprise-wide visibility to network traffic flow data.

The network traffic flow data is used for multiple purposes. First, it is used in combination with specialized tools to identify devices with similar functions (for example: IoT systems, bio-med and imaging devices). These devices are discovered using segmentation tools which give the necessary visibility to enable populating enclaves with IP addresses.

Stealthwatch and Tetration can also be used to audit enforcement policy. By comparing observed network behavior derived from flow data to define policy, the specialized segmentation tools can confirm if the deployed policies are in fact being enforced as expected. For auditors, this provides valuable insight that can accelerate the audit process.

For the internal SecOps team, the ability to audit enforcement policy provides key assurances that segmentation policies are effective at reducing the attack surface area and enterprise security risk. Finally, specialized segmentation tools can create or modify enforcement policy files, created for specific enforcement platforms. These files can then be pushed to these platforms.

Security Monitoring and Optimization Services

Deployment of segmentation policies is not the final step in the segmentation process. Ongoing management, control, and optimization of the deployed (visibility) technologies and segmentation policies are critical for overall security. Cisco views segmentation as a continuous process, and thus, requires ongoing monitoring. As networks change over time, gaps can emerge in the segmentation strategy.

Using tools like Stealthwatch and/or Tetration to monitor actual observed network traffic and comparing it to published policy helps to quickly identify these gaps. The sooner gaps are identified, the sooner they can be addressed with adjusted segmentation policies, thus reducing risk. In addition, visibility and segmentation technologies can vastly increase the telemetry fed to the client's security operations center (SOC) and expand breach response options.

Clients that have long-term compliance requirements will be able to use the data produced by the specialized segmentation tools as evidence for compliance teams.

Cisco Security Segmentation Services Approach Summary

1. The framework starts with **Cisco Security Advisory** Services team. In this phase, experienced security engineers work with the client to understand their business objectives and craft a segmentation strategy that closely aligns with those goals.
2. Cisco works with each client to build repeatable design patterns for consistent asset identification and classification based on clearly defined characteristics.
3. Cisco then works with each client to understand, develop and implement a strategy for collecting network traffic (NetFlow, SPAN) based on tools such as Cisco Stealthwatch with specialized segmentation capabilities for campus networks and Cisco Tetration for datacenter visibility.
4. Network visibility allows for segments to be properly defined, asset placement validated and trusts understood by leveraging Cisco Stealthwatch and Cisco Tetration to populate segments with the appropriate network endpoints.
5. The information gathered about the network and devices results in identification of the most critical enterprise assets. Deeper analysis of the visibility report is performed to help build segmentation policies and, in consultation with the data/system owners, to define allowed traffic.
6. Followed by policy enforcement that employs the new and existing enforcement technologies. At this stage, the **Cisco Security Implementation Services** segmentation team will begin the infrastructure and segmentation tool deployment.
7. Detailed designs which reflect the network infrastructure needed to mirror the segmentation architecture are created and deployed. Deeper technical knowledge transfer (KT) on as-built design and run-books help aid the client's "Day-2" operational readiness.
8. Once deployed, ongoing operations would be defined for segmentation audit and policy updates. The Day-2 operating model defines a governance process that includes new segment intake, IT service management process, and separation of duties. This also includes integration of new security telemetry into the enterprise SOC.

Contact

For more information and to speak with a security expert, please contact us.

Learn more about Cisco Security Services.

