Group-Based Policies for Zero-Trust Security

Contents

Overview

Network policy is a collection of rules that govern the behavior of network devices. Just as a federal or central government may lay down policies for states or districts to follow to achieve national objectives, network administrators define policies for network devices to follow to achieve desired business outcomes.

A network that follows well-defined policies capably fills business needs that it is designed to support. Think of network policies as objectives or goals. Without clear objectives, your network can't be set up to deliver optimally, and without goals, its performance can't be measured.

Since network policies specify how the network must function in different circumstances, there is no predefined list of policies. A network's policies depend on what's necessary to achieve each business's objectives. Some of the more common policies that all businesses need to consider are access and security, application and QoS, traffic routing and service insertion, etc.

As organizations increasingly adopt a zero-trust security framework, defining and enforcing effective access policies becomes ever more important. Policies for zero-trust security require all users inside and outside the organization's network to be properly authenticated and authorized according to the rights and privileges they enjoy to access organization's data and application. Properly written policies can prevent unauthorized access to sensitive information and can serve as the basis for effective segmentation of the network, which can, in turn, minimize the spread of malware and help reduce risk. On the other hand, erroneous policies can hinder the smooth functioning of the organization. Therefore, accurate definition and enforcement of access policies is critical to all organizations.

Policies play a central role in Cisco Digital Network Architecture (Cisco DNA), an intent-based network. Business intent is captured and translated as network policies that drive automation, assurance, and security, making the network more intelligent and better able to achieve business objectives. In this paper we shall consider the importance of access and security policies in Cisco DNA and how they form the basis of zero-trust security.

Intent-based networking and the role of policies

Modern organizations are realizing that because of the proliferation of user and IoT devices, increase in user mobility, expansion in cloud applications, and above all, increased need for security, their legacy networks are not going to provide the level of service they need. Older, manual ways to onboard devices, configuring each port of the switch they connect to, and setting up their access control through firewalls and access control lists (ACLs) is no longer feasible. The network needs to get smarter by increasing automation, providing the requisite security, and optimizing the level of service, to step up to these modern challenges.

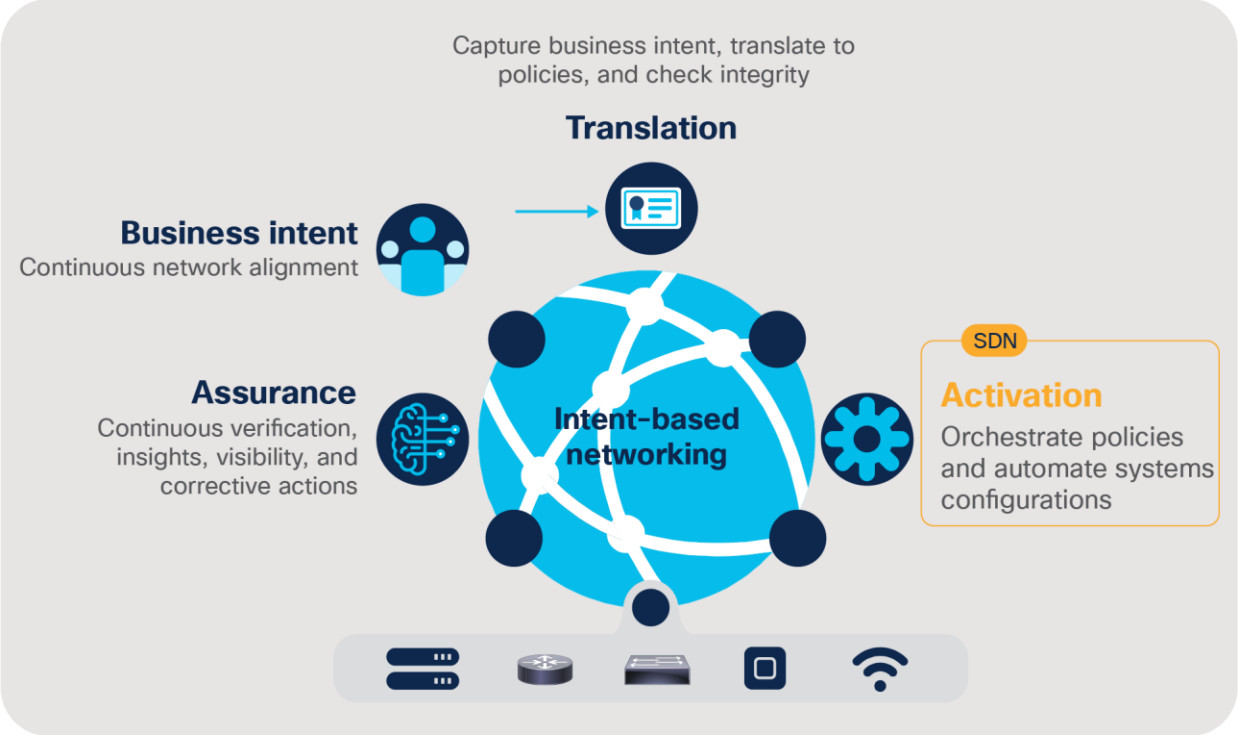

Figure 1.
Intent-based networking starts with translating intent into network policies

Intent-based networking (IBN) is an industry-accepted framework that lets networks do just that. IBN transforms a hardware and CLI-centric, manual network into a controller-led network that captures business intent and translates it into policies that can be automated and applied consistently across the network. The goal is for the network to continuously monitor and adjust network performance to help ensure desired business outcomes.

Cisco DNA is Cisco's implementation of intent-based networking for access and WAN networks. It is an open, extensible, software-driven architecture that accelerates and simplifies your enterprise network operations, while lowering costs and reducing your risk. Cisco DNA is a controller-directed architecture in which Cisco DNA Center is the central control point for all network activity. Cisco DNA Center is crucial for network abstraction that lets IT treat the network as an integrated whole. The functioning of Cisco DNA is driven by policies defined in Cisco DNA Center. These policies include those for access, routing, quality of service (QoS), etc., and are used by Cisco DNA Center to configure the network infrastructure for achieving the desired outcomes.

Policies are really at the heart of effective functioning of every Cisco DNA-based network. Policies control how network devices are configured, how virtual network topologies are built, what quality of service levels are provided to each application's traffic flows, and how users and things are authenticated and authorized before being allowed to join the network.

The complexity in defining access policies

As a security decision maker, how would you determine access policies that are right for you? You probably already have a good idea – you would obviously not want your network to let IoT devices access your financial records or your customer database, but you would give such rights to your accountants and salespeople, respectively.

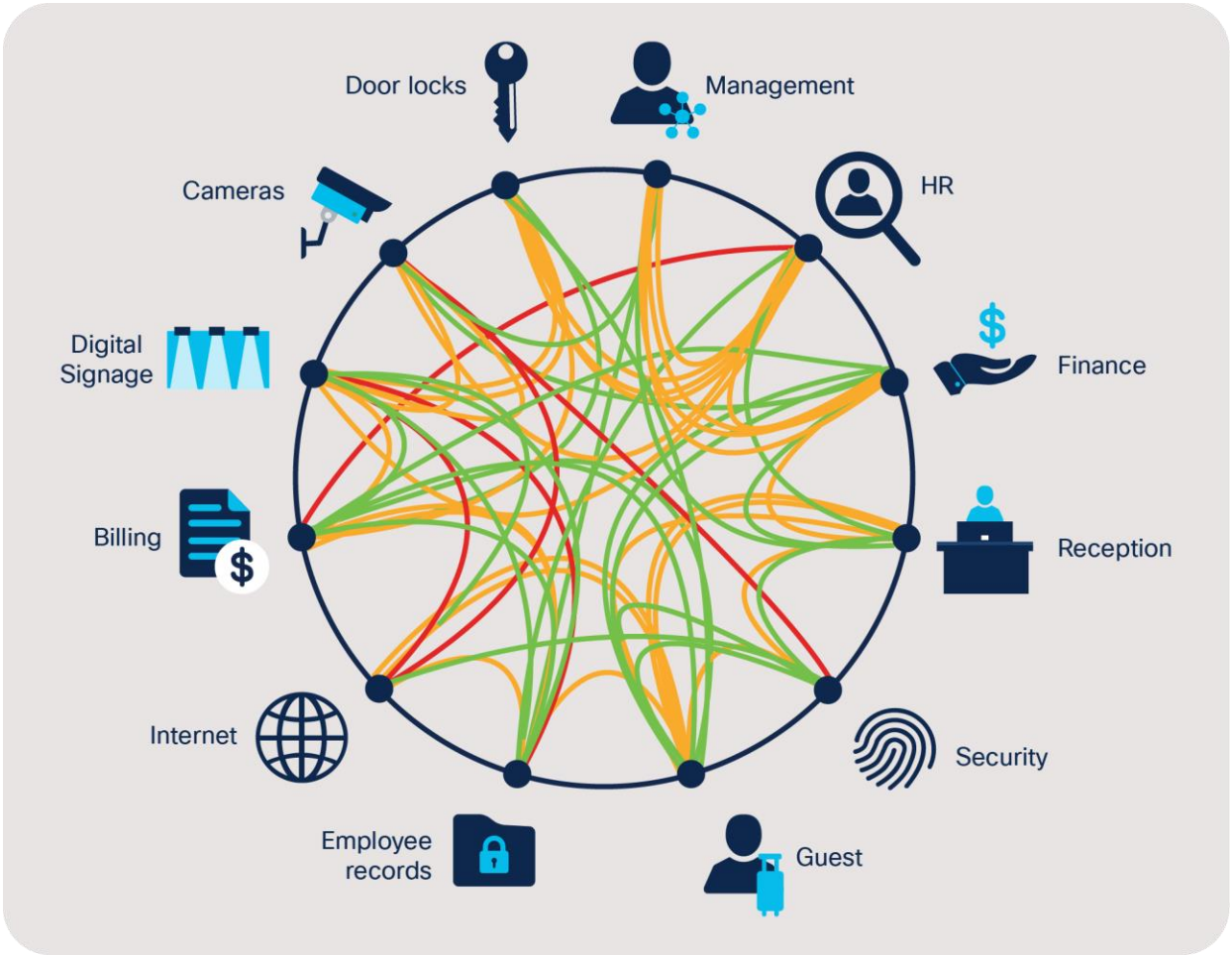

Figure 2.
Defining effective access policies can be complex

But can you craft your access and segmentation policies only on broad generalizations? There can be nuances. For example, you might want to provide access to your HR personnel only when they are securely connected to the office network and not when they connect from the local coffee shop. Figure 2 illustrates how complex these access control policy definitions can become.

For defining a comprehensive access policy, you need to know how users and devices in your network interact with each other so your security policies can allow legitimate traffic and block the rest. Intuitive knowledge gives you a start, but not fine-grained control, because a lot of interactions may be hidden from you, and if you don't account for them properly, you can impede your normal expected operations.

Policy functions within Cisco DNA Center can help. These functions help you discover, define, and author effective and rational access control policies, and, with the help of Cisco® Identity Services Engine (ISE), enforce them through the underlying network infrastructure.

Group-based policies and zero-trust security

Access control policies based on IP-addresses or users' locations are not manageable or scalable. Imagine a scenario where you need to write several lines of IPACLs for every user or thing based on the IP-address at the time and configure firewalls to allow or deny their access to sensitive data based on each application to be used. Now consider doing this for thousands of users, figure out where they are joining the network from, and from which device, and account for their moving from location to location – and you can see how quickly it can get out of hand.

```
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny udp 130.237.66.56 255.255.255.255 lt 3943 141.68.48.108 0.0.0.255 gt 3782
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255 gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt 3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243 255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255 eq 3721
access-list 102 permit tcp 126.97.113.32 0.0.1.255 eq 4644 2.216.105.40 0.0.31.255 eq 3716
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq 4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
```

Figure 3.
Defining access policies based on individual IP addresses

Group-based policies can help. Instead of applying every policy to each endpoint, you apply them to a group of users and/or things simultaneously.

```
DMZ-Pod1#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 4:Employees to group 12:Development_Servers:
       Deny IP-00
IPv4 Role-based permissions from group 8:Developers to group 12:Development_Servers:
       Permit IP-00
```

Figure 4.
Group - and role-based ACLs

Group-based policy provides you with a business-focused way to manage access control. You're equipped with a single stop to visualize security policy functions. This capability on Cisco DNA Center works with ISE as the policy engine and the network infrastructure as the enforcer and provides you with the tools to manage policies independently of your network design and topology with an approach that can scale seamlessly.

The result of applying group-based policies is segmenting the connected endpoints (user and smart IoT devices) on your network into scalable groups and tagging their communications, such that the packets can be easily identified and tracked as they traverse the network. Such tagging lets you create a much more intuitive and easier way to express policies. For example, now, instead of writing thousands of ACL statements in your switches, you can simply say, "Allow accountants on their corporate laptops access to company sales applications and data, while denying the same accountants access to this sales application from their personal phone." There is no need for IP addresses, no dependency on where the accountants are, and it doesn't matter whether you have one accountant or a thousand.

Group-based policies provide the basis for network segmentation. Once you have established logical groupings for all your users and things, provided you have the support from the underlying network infrastructure, you can permit or deny each group access to protected resources. This access control policy is a key part of zero-trust security for the workplace.

Table 1. Zero-trust for the workplace: threats and solutions

Threat	Zero-trust solution	Cisco group-based policy implementation
Unauthorized endpoints or devices with an unhygienic posture can disrupt productivity.	Authenticate and evaluate system health (no network access until endpoint trust is evaluated)	**Visibility:** Fully identify and profile endpoints with continuous verification through behavioral analytics
Noncritical assets with unrestricted network access can make the entire infrastructure vulnerable.	Provide confined access to essential services through macro- and microsegmentation.	**Segmentation:** Define, author, and enforce access policies for effective network segmentation
Compromised endpoints can infect other assets in the network through lateral movements.	Continuously evaluate trust and apply adaptive controls to isolate threats in real time	**Containment:** Continuously verify endpoints and policies through behavioral analytics; quarantine endpoints with anomalous behavior

Zero-trust security for the workplace restricts communication based on least privilege, granting only the minimum level of system/network access rights to people and technology that will enable them to carry out their missions as required by business objectives. This approach is critical in supporting a zero-trust framework and benefits the organization by reducing overall risk, shrinking the scope of compliance, and limits the lateral movement of malware to contain threats like ransomware.

For decades, network segmentation has been a well-known best practice, but the underlying technology has been very complicated and error prone. In a large network with many clients and network devices, it becomes extremely complex to section off routes using firewalls and manually configuring ACLs. That difficulty often stops many organizations from tackling segmentation projects.

Cisco group-based policy approach to network segmentation helps you realize zero-trust security.

Five-step group-based policy journey in Cisco DNA

To help you through your policy journey, Cisco DNA Center in combination with ISE provides you with policy management and analytical insights to define, author, and enforce effective policies. These steps are part of the Cisco Software-Defined Access (SD-Access) solution. Cisco SD-Access uses group-based policies to build an automated secure switching fabric that is uniform across wired and wireless networks. An SD-Access-created switching fabric is standardized, fully automated, and scalable, and it enforces all group-based access policies for connecting endpoints.

1. Cisco AI Endpoint Analytics

Definition of access policy in Cisco DNA Center starts by identifying and profiling all endpoints (IoT and user devices) connected to the network. Accurate identification and complete profiling are important to determine their role so appropriate policies can be applied. Figure 5 shows how endpoints that were only known by their IP and MAC addresses on the left are analyzed through a process involving collection and aggregating data from many sources including Deep Packet Inspection (DPI), telemetry, user inputs, configuration databases, and external sources, analyzing the collected data, and applying machine learning (ML) technologies to completely identify the endpoints on the right.

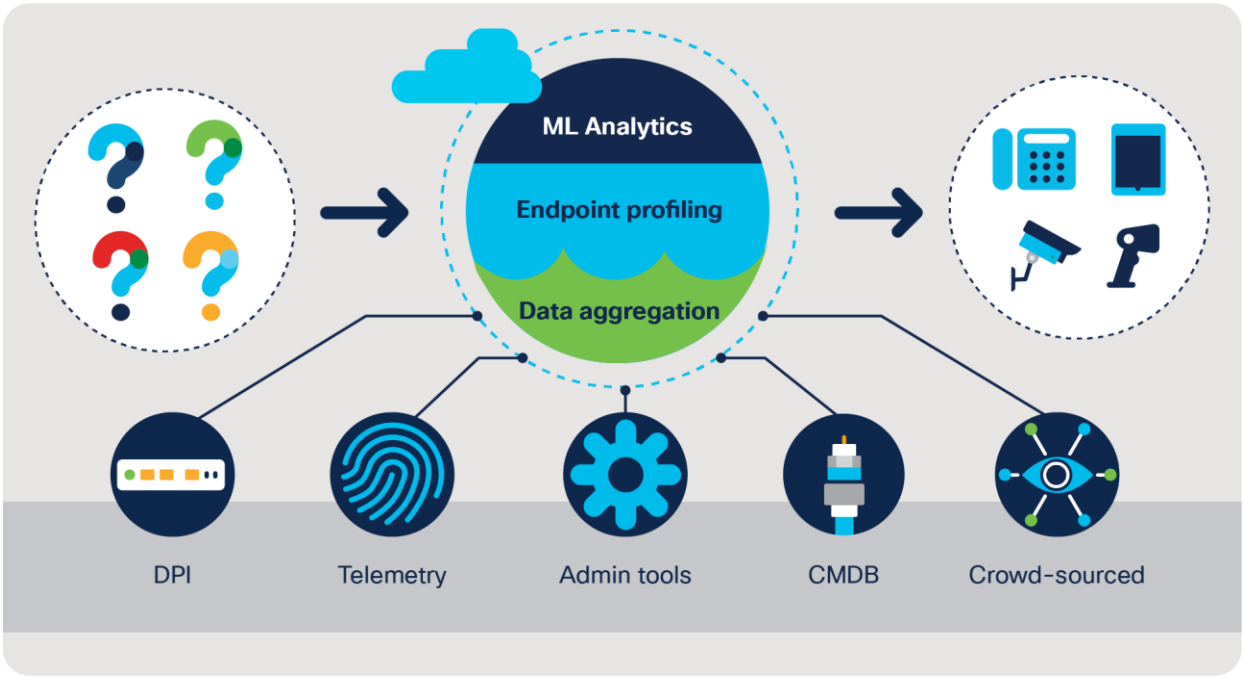

Figure 5.
Cisco AI Endpoint Analytics identifies, profiles, and groups endpoints

Their accurate identification allows similar endpoints to be placed in groups, which forms the basis for defining policies.

2. Group-based policy analytics

Next, Cisco's group-based policy analytics gives you the detailed information you need to define and enforce effective access policies. It gathers and analyzes actual traffic flows and presents a visual flowchart with information on service, protocol, and ports used between pairs of source and destination groups.

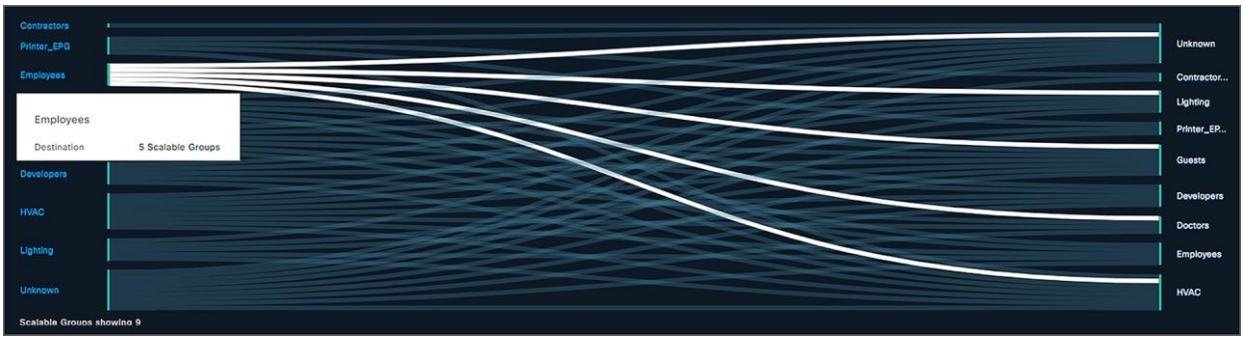

Figure 6.
Group-based policy analytics provides a visual analysis of traffic flows between groups

Group-based policy analytics starts where Cisco AI Endpoint Analytics leaves off. It uses endpoint groups that AI Endpoint Analytics creates, along with groups from ISE and Cisco Stealthwatch®.

Group-based policy analytics melds your view of groups with traffic flows. This provides insight into which groups are engaged with which others, better positioning you to assess the right policies for your environment. By discovering your existing scalable groups and their corresponding traffic based on NetFlow information, you can understand with greater depth, not only which groups are communicating but also the ports and protocols, leading to a clear understanding of the communication needs between groups or the lack thereof. This unique insight can be crucial to your policy decisions as you translate your business needs into meaningful policies. Protecting your corporate assets with business-intent-based policies has never been easier.

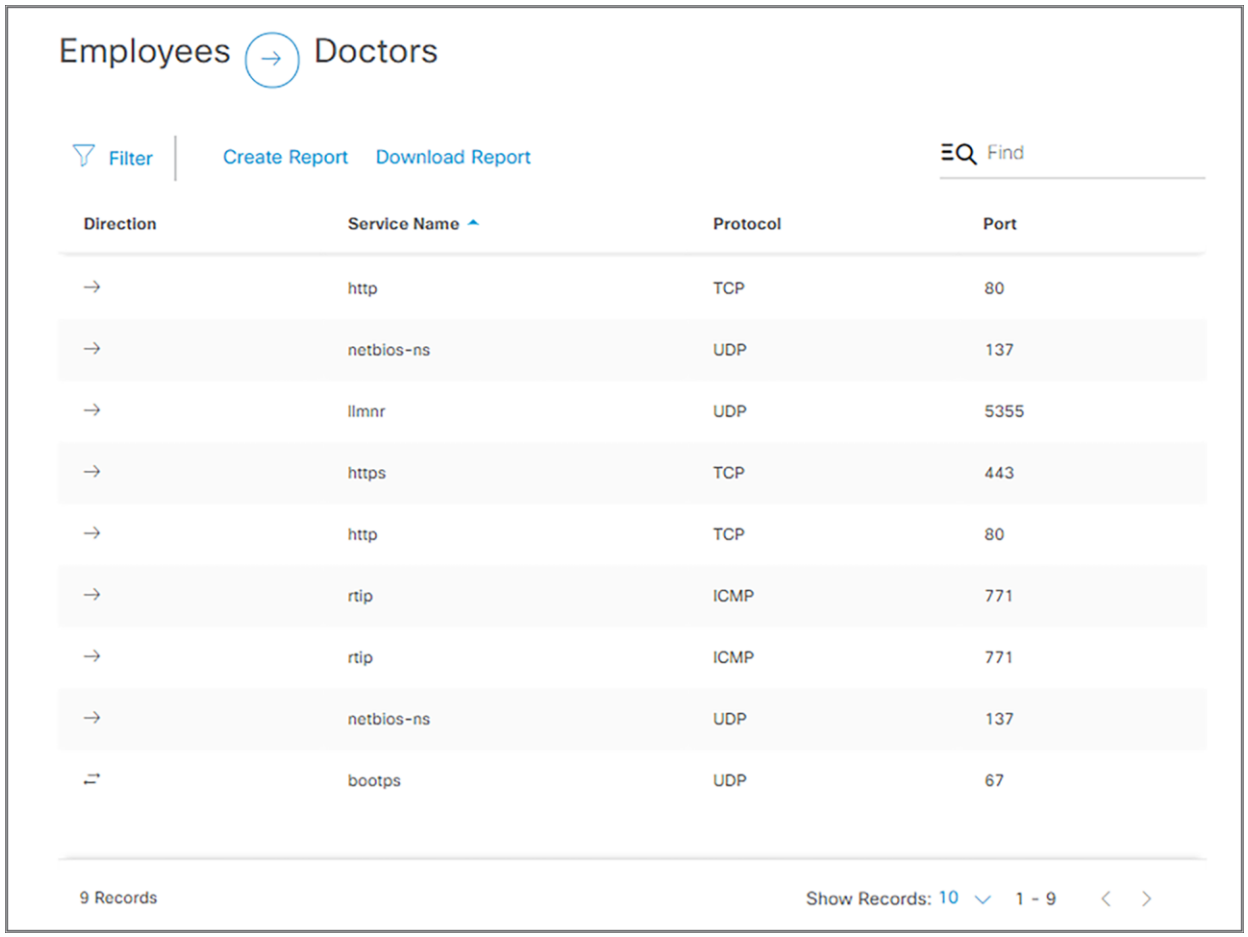

Figure 7.
Group-based policy analytics provides detailed traffic insights

Seeing traffic interaction of scalable groups with ISE profiles and Stealthwatch Host Groups can help you visualize potential security risks and lead to a clear understanding of new scalable group needs.

3. Group-based access control

Once we figure out the right policies, we need to get them into the network so the network infrastructure can begin to enforce them. This is where we use group-based access control (also known as Access Control Application), another feature built into the Cisco DNA Center. This feature presents an easy-to-use matrix with endpoint groups as sources and destinations on its X and Y axes, and with each cell of the matrix representing the policy, down to the service, transport protocol, and port levels, that governs communication between them. Such a matrix makes defining granular interaction policies between groups simple, and the whole process scalable.

Figure 8.
Group-based access control provides a visual matrix for easy policy representation

Group-based access control sends policies to ISE, which functions as the security policy engine for the solution. ISE dynamically programs the network infrastructure – switches, routers, wireless access points, and LAN controllers, so they can enforce these policies. All packets from and to endpoints are now appropriately tagged, placing the endpoints into the right network segment.

4. Uniform network fabric

Once segmentation based on access policies is enforced, network overlays are created. Overlays are virtual networks that can be thought of as multiple independent networks based on the same physical infrastructure, each of which connects just the users and resources that can communicate with each other. Cisco SD-Access creates the switching fabric necessary to build these virtual overlay networks.

The switching fabric created by SD-Access uniformly applies group-based policies no matter how or from where the user or IoT endpoint connects– wired, wireless, or VPN – easing administrative burden and enhancing user mobility. It standardizes network configurations. Standard configurations make scaling the network easy. By using verifiable policy-based segmentation that keeps traffic from different groups apart, an SD-Access switching fabric improves regulatory compliance and risk management. Placing limits on where traffic from devices can travel, the fabric limits the scope and helps contain threats. The fabric's segmentation allows infected or untrusted endpoints to be quarantined.

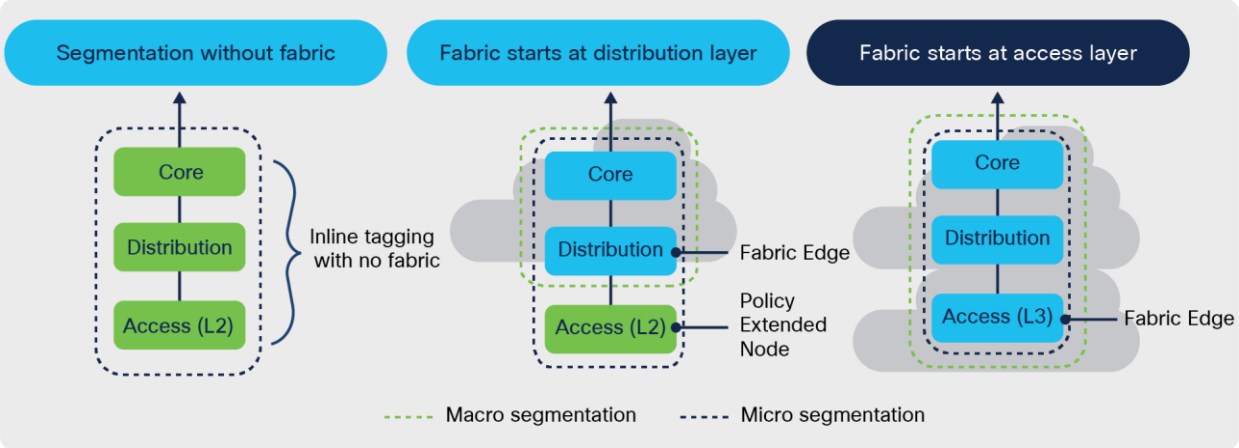

Figure 9.
Gradual migration of an existing network to a network fabric using policy-extended nodes

SD-Access provides a way in which a fabric can be built gradually over an existing traditional network. In the first step, you can use templates in Cisco DNA Center to segment the network without manual configurations. This step allows you to use the power of group-based policy constructs without a fabric. As a next step, you can introduce the fabric in just the core and distribution layers of the switching topology. In this way the existing virtual LANs (VLANs), ACLs, etc., of the network are preserved and users and devices connected to the access switches experience no disruption. Access switches may enforce group-based policies using the concept of policy-extended nodes in which these switches provide fabric benefits while still maintaining Layer 2 access. Access switches and their users can then be migrated over to the fabric one by one while maintaining full backward connectivity during the process.

5. Group-based policy over multiple domains

An enterprise network needs to deliver end-to-end services to users, things, and applications. However, the enterprise network itself is likely built with several separate technology and administrative constituent networks or domains. Typically, each constituent network is designed, provisioned, and optimized for its own purpose and business objectives, such as campus and branch network for access, WAN to connect campus and branches with data centers and clouds, and data center networks for running workloads and applications.

Cisco multidomain integration seeks to use uniform policies in all the enterprise's constituent domains. Integration of policies between domains allows policies to be defined once and applied coherently across the enterprise.

For example, integration of group-based policies in SD-Access with those in Cisco Application Centric Infrastructure (Cisco ACI®) creates an end-to-end segmentation that extends role-based access from the campus to the data center and clouds. Similarly, extending group-based polices from SD-Access in the campus to branches across SD-WAN creates a uniform, secure enterprise-wide network that allows user mobility throughout without compromising on access privileges.

Conclusion

No matter where you are in your policy journey, Cisco DNA Center's group-based policy features can help you develop and manage policies with greater confidence and ease. Group-based policies can help reduce your operational efforts and enable you to make faster policy changes and reduce risk to the business. Use the following references as your next steps and to get started with securing your network with group-based policies.

- Understand what network policy is: What is network policy?
- Read how to use Cisco DNA Center applications to define and enforce your access control policies: Write policies for right segmentation
- Get practical advice on segmentation: A prescriptive guide to segmentation strategy
- Video repository on group-based policy: Cisco Group-Based Policy
- Get technical guidance on deploying group-based policy analytics: Group-Based Policy Analytics Deployment Guide
- Get more information on SD-Access: Read the solution overview

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-744416-01 01/21