Cisco
The bridge to possible

Common Policy Is Uniquely Cisco

Network administrators have a problem in the post-pandemic world: namely, access patterns have changed. Many users are operating in a hybrid model and on any given day can log in from different locations. These locations can run the gamut from remote to the office, from either the campus or the branch. Zero-trust access from anywhere requires consistent segmentation and access policies among users, devices, and application workloads regardless of whether they are remote or on-premises. How does an administrator secure users and agentless devices—both OT and IoT—as they come on the network and are communicating with applications on-premises, in a cloud service provider, or on the internet?

Depending on where you choose to enforce the policy, each domain has its own structure for implementing access and segmentation policy, and these domains are not all speaking the same language. For example, when it comes to WAN, it is all source and destination IP address. When creating static policies using IPs, rules are meaningful when first added. But things change, and old entries are never removed. As a result, an administrator doesn't know if it's a corporate employee logging in from a corporate laptop or a contractor logging in from their own device.

To complicate matters even more, in a multi-domain, multi-siloed network it can be difficult for each part of the network to speak and understand the same language. For example in the Application Centric Infrastructure (ACI) world, communication is not through Security Group Tags (SGTs), rather it's with Endpoint Groups (EPGs) and Endpoint Security Groups (ESGs). The question that needs to be asked is: how do you share application workload context with other domains if they don't understand one another?

That's where Common Policy steps in. Think of Common Policy as the universal translator that connects the entirety of your network through one consistent language. Available in Cisco Identity Services Engine (ISE) 3.4, this release allows for a holistic strategy of cohesiveness covering all aspects of the network.

How does it work?

Common Policy provides the solution to the network administrator's problem. Context information is created closer to the domain where it resides: the access layer for users and devices and in the data center or cloud for application workloads. This context is normalized to a group construct, namely a Security Group Tag (SGT), that is understood across all of the domains.

The normalized user, device, and app workload context is sent to each domain using Cisco ISE as the exchange hub.

This enables security administrators to create consistent access and segmentation policies regardless of which domain they choose to enforce policy.

Make no mistake, Common Policy is not a new pane of glass solution. But since Cisco ISE already has one of the industry's largest ecosystems for context sharing, customers can get value from this solution from Day One.

One of the biggest changes is the enhancement of the existing Cisco ISE integration with ACI that will now be multi-pod, multi-tenant, and multi-VRF (Virtual Routing and Forwarding), making it the perfect solution for larger customers. It's no longer a worry that ACIs use different languages like End Point Groups (EPG) or Endpoint Security Groups (ESG). Thanks to Common Policy, it becomes easy to translate incoming EPGs and ESGs into SGTs in Cisco ISE so that other domains have the exact same structure to work from.

Sending context and enforcing policy on ACI has improved as well. SGTs can be translated into external EPGs and be assigned contracts all from within Cisco ISE. Common Policy allows the ecosystem to expand so that application workloads can be brought in from external on-prem and cloud providers with VMWare, AWS, and Azure. Within Cisco ISE customers can assign these workloads to SGTs and then send them out to other domains–including ACI–to use in building access and segmentation policies.

Further your zero-trust initiatives

Common Policy extends zero-trust-based access to Cisco and other network domains by gathering context, storing it, and sharing it with other controllers. Furthermore, Common Policy learns new groups and shares context using granular filters.

Sharing this context now enables NetOps and SecOps to choose the domain of their choice for policy enforcement based on whichever domain they feel they need to have that control on. They could even choose to implement policy in multiple places. Cisco is providing the flexibility to build those policies with the consistent context enabled by this solution.

Learn more

Click to learn more about Cisco ISE.