Cisco IT Insights

Dynamic Policies to Control User Access

What

When Cisco sold a portion of its video business to Technicolor in 2015, some of the transferred employees still needed access to certain resources on the Cisco network. These employees would be working in Cisco offices—located in Shanghai, China, and Lawrenceville, Georgia—until they transferred to Technicolor offices or the offices were turned over to Technicolor. In the meantime, we needed a secure, economical way to give these employees defined access to the Cisco network and its resources from the Cisco offices.

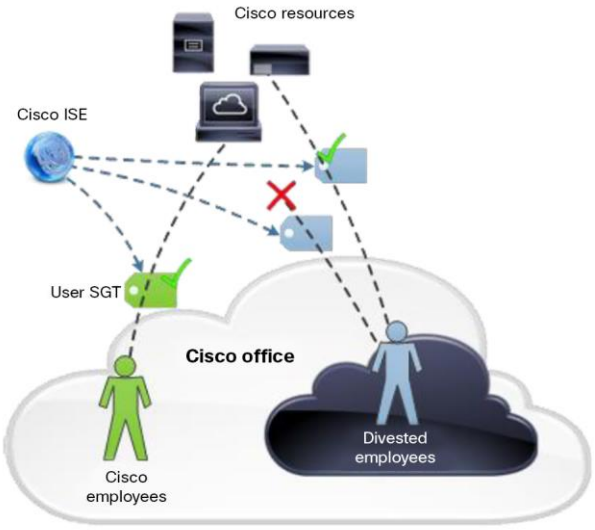
We wanted to provide this segmented access through a logical separation in the network infrastructure, instead of the costly and cumbersome effort to add dedicated circuits to our nearest network hubs. We also wanted to make sure these users would not be able to get full network access simply by plugging into a wired port in a Cisco office.

To meet these requirements, we developed a new solution called dynamic user policy. The policy uses access control capabilities in the Cisco® Identity Services Engine (ISE) and the security group tagging feature in Cisco TrustSec® technology.

With dynamic user policy, we configure policies on the Cisco ISE to define which Technicolor users are authorized and which applications (e.g., email) and resources (e.g. Cisco WebEx®) they can access on the Cisco network. By basing access permissions on username, the dynamic user policy approach provides granular security that follows the user, enforcing the same policies regardless of where the user connects to the Cisco network.

When a Technicolor user logs in to a switch or network gateway in a Cisco office, that user is authenticated. Then all of the user's data receives a security group tag (SGT) identifying it as coming from the Technicolor group. Permissions and restrictions defined on the associated access control list (ACL) are applied by the Cisco ISE at that point (Figure 1).

Figure 1. User Access Based on Security Group Tags



Similarly, all network resources (e.g., a particular Cisco TelePresence® endpoint) also have tags, which can be included in the policy for a particular security group. Users and resources can be configured into any security group based on the needs of the organization. If a user tries to log in and has not been associated with a group, the user will be placed into a default “untrusted” group, which has a policy that is defined to severely limit access to network resources.

Why

The security group tag follows a user across the network for consistent, flexible, dynamic, and scalable security. By defining permissions and restrictions according to username, the dynamic user policy method adapts more easily to policy changes than methods based on IP address.

In the future, we will be able to extend this method to other types of users, such as on-site vendors and contract employees who need limited access to certain resources and applications on the Cisco network.

Dynamic user policy will also help us reduce costs by limiting dedicated circuits to locations where they serve ongoing work by a large number of users.

For More Information

Cisco Identity Services Engine

Cisco TrustSec

To read additional Cisco IT case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described. Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

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 www.cisco.com/go/offices.