Cisco Context-Aware Secure Access (Security Group Tags [SGT])

Technology Postcard

Customer Need: Scalable, Simplified Access Policy Enforcement

Many types of devices, including laptops, smartphones, and tablets, are used by end users to connect to the network wired, wirelessly, and remotely through VPN. With bring your own device (BYOD) access, the devices can be personal or corporate owned. Every enterprise has policies that dictate who can access what applications and databases, when and how. Traditionally, IT manages the policy either by introducing appliances at points in the campus where users connect or by manually configuring all the access switches. Appliances incur additional capital and operational expenses, whereas manual configuration of the switches requires maintenance of every switch. Moreover, the network can carry traffic using Ethernet, IPv4, IPv6, or other technologies, so the configuration must keep up with changes in technology, which leads to higher operational complexity and costs.

Feature Description: Security Group Tags

Cisco Security Group Tag (SGT) is a technology, part of Cisco SGA/TrustSec architecture, that overcomes the shortcomings of the traditional approaches to policy administration. When a user connects to the network and tries to access an application, the Cisco access switch automatically profiles the user and finds out the user's ID, device being used, location, and time of access. The switch then tags all traffic coming from the user's device based on the IT policy for the user's profile. The tag is a numerical value and is either manually assigned to the access switches or automatically administered through the Cisco Identity Services Engine (ISE) application. If Cisco ISE is used, it transmits the tag information to all the supported Cisco devices in the network. Every packet from the user's device is tagged. Decisions based on the tag can be taken by any switch in the network. Typically, the switch connected to the server where the application or database resides enforces access based on IT policy. The user's request will either be allowed or denied. Here is a use case that shows the benefits of Cisco Security Group Tag.

Use Case

- **Without Cisco Security Group Tag:** In order to provide access based on employee role, IT manually administers policy using an access control list (ACL) in all the access switches in the network. The staff does this for each employee role. After this is done, if a marketing person attempts to access a restricted financial application/database, these ACLs will deny the request. A change in role or policy will result in IT reconfiguring the policies in all the switches. Moreover, ACL is tied to the IP address, and IP addresses change, breaking the policy (for example, when a marketing user in the United States travels to Europe and is able to access the financial application).
- **With Cisco Security Group Tag:** IT will set up the access policy in Cisco ISE stating that the marketing group cannot access the financial application. When the marketing person connects a laptop/tablet to the network, ISE uses Active Directory credentials to authenticate the user. ISE then assigns a tag, say, 20 for the marketing group. The access switch receives the tag 20 from ISE and adds it to every packet coming from the user's device. The packet traverses the network with the tag 20. If the user attempts to connect to the financial application/database, which only allows a tag of 30, the access switch connected to the server will deny the request. If the marketing user switches the role to finance, that user's user group will change based on Active Directory, and the application can be accessed without IT having to program all the access switches. The entire authentication and enforcement process is automatic.

Benefits

1. Scalable as ISE maintains a single database of all tags and related access policies. Without SGT, IT is handicapped with a few policies and those that are dependent on specific network topology.
2. IT has the option of manually setting the tags (for example, in a small firm) or using ISE. With ISE, employees can move and change departments requiring only one change in ISE or Active Directory.
3. Not dependent on the type of network (Layer 2, IPv4, IPv6), so it is an effective mechanism to roll out identity-based access policies across the entire network.

Supported Catalyst Platforms

- Cisco Catalyst® 6500
- Cisco Catalyst 4500E
- Cisco Catalyst 3750-X
- Cisco Catalyst 3560-X

For More Information

www.cisco.com/go/trustsec

www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11640/white_paper_c11-663616.html

C22-722459-00 01/13