CISCO VALIDATED DESIGN

User-to-Data-Center Access Control Using TrustSec Design Guide

October 2015

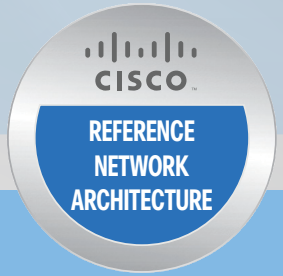


Table of Contents

About This Document

This document describes how Cisco TrustSec provides access control for user to data center (“north to south”) traffic for wired and wireless users. Cisco TrustSec provides software-defined segmentation and enables role-based security policy.

Tech Tip

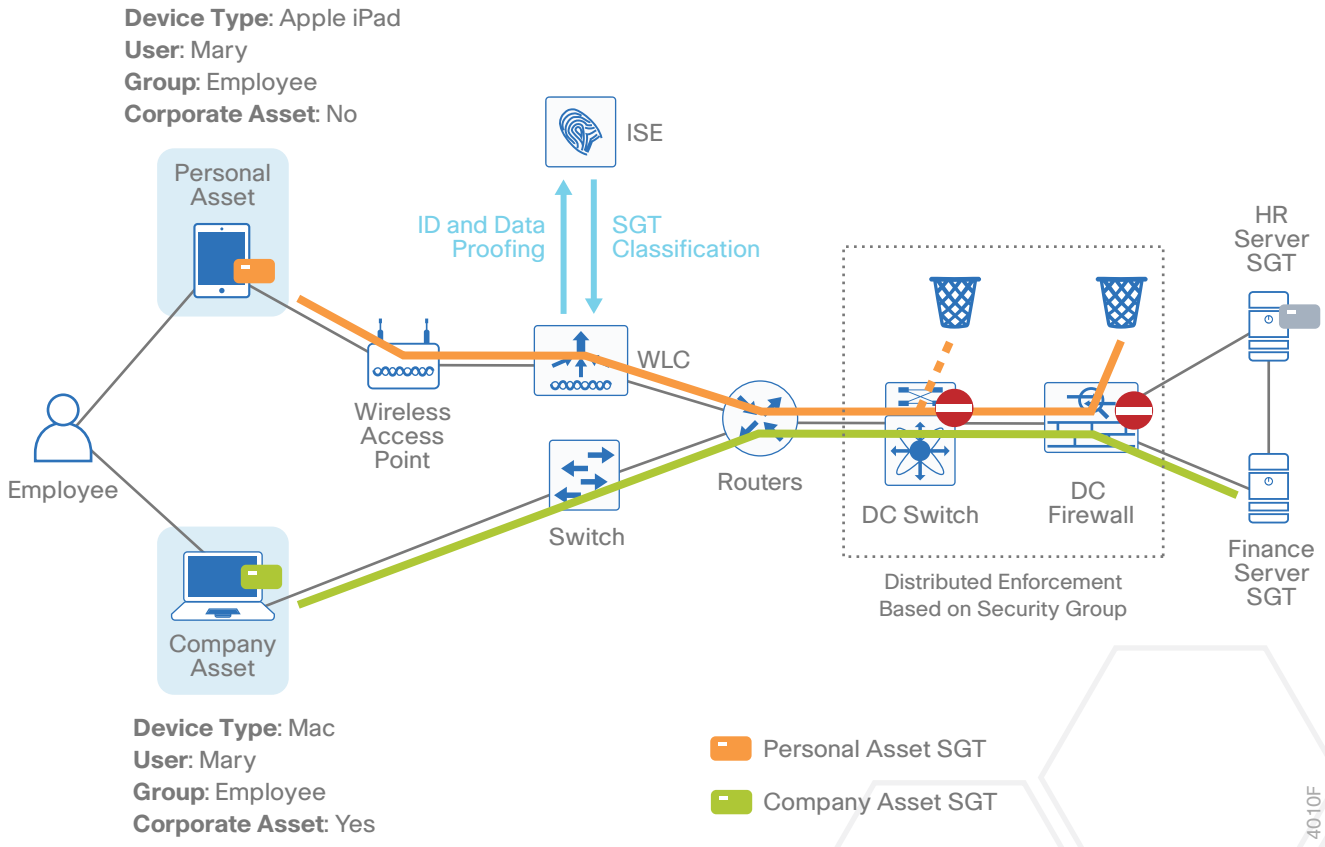
For more information about Cisco TrustSec, go to:
http://www.cisco.com/go/trustsec

Cisco TrustSec Overview

The Cisco TrustSec solution simplifies the provisioning and management of network access control through the use of software-defined segmentation to classify network traffic and enforce policies for more flexible access controls. Traffic classification is based on endpoint identity, not IP address, enabling policy change without network redesign. A centralized policy management platform gathers advanced contextual data about who and what is accessing your network, uses security group tags (SGTs) to define roles and access rights, and then pushes the associated policy to your TrustSec-enabled network devices, such as switches, routers, and security equipment. This provides better visibility through richer contextual information and allows an organization to be better able to detect threats and accelerate remediation, reducing the impact and costs associated with a potential breach.

Cisco TrustSec technology is embedded in Cisco switches, routers, and firewalls and is defined in three phases: classification, propagation, and enforcement. When the user's traffic enters the network, the traffic is classified based on the results of authentication, such as 802.1X, MAC authentication bypass, or web authentication. After the user's traffic is classified, Cisco switches and routers then propagate the traffic automatically, without any intervention by the network operator until it hits an enforcement point, which can be a Cisco firewall, router, or switch. Based on the classification, the enforcement device determines if the user's traffic should be allowed or denied.

Figure 1 *Cisco TrustSec phases: classification, propagation, and enforcement*



Use Cases

RETAIL: SEGMENTATION FOR PCI COMPLIANCE

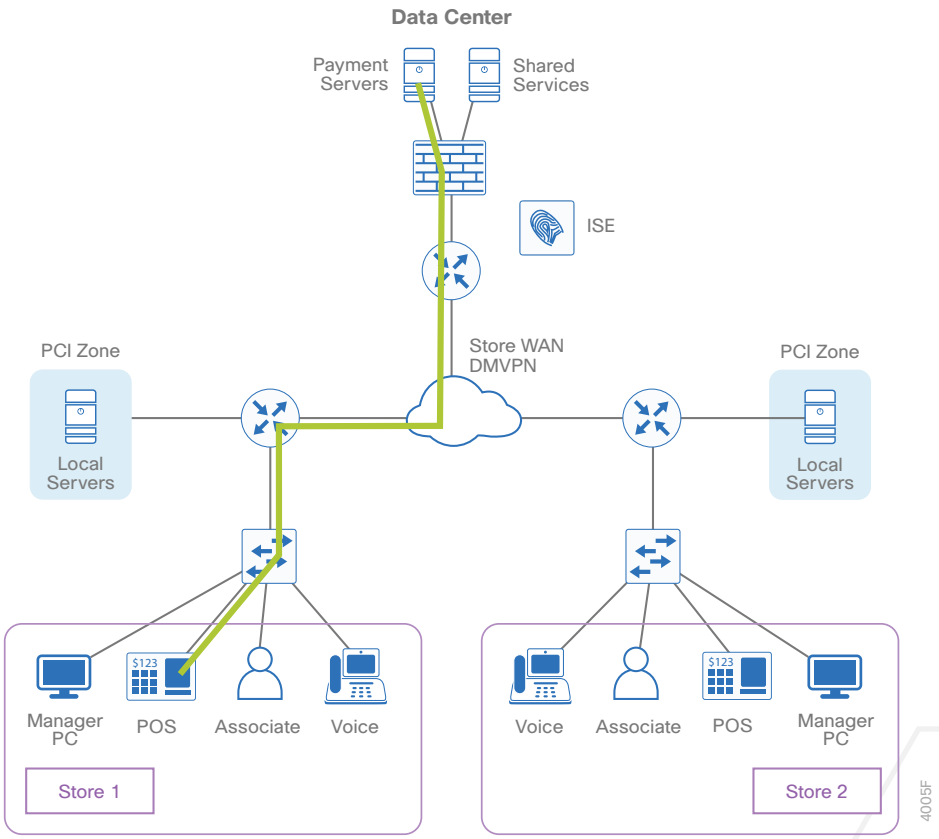
Business Problem

A retail chain is required to comply with Payment Card Industry (PCI) standards where all devices that process credit-card information are in a network that is segmented from other devices.

Solution

The PCI devices are tagged by the switch or router at the store and provided access to the payment servers in the data center, which is enforced at the data center by a data center switch or the data center firewall. The devices on the network that aren't used for processing payment information get an appropriate tag that prevents them from accessing the payment servers but allows them access to shared services provided in the data center.

Figure 2 *TrustSec for PCI compliance*

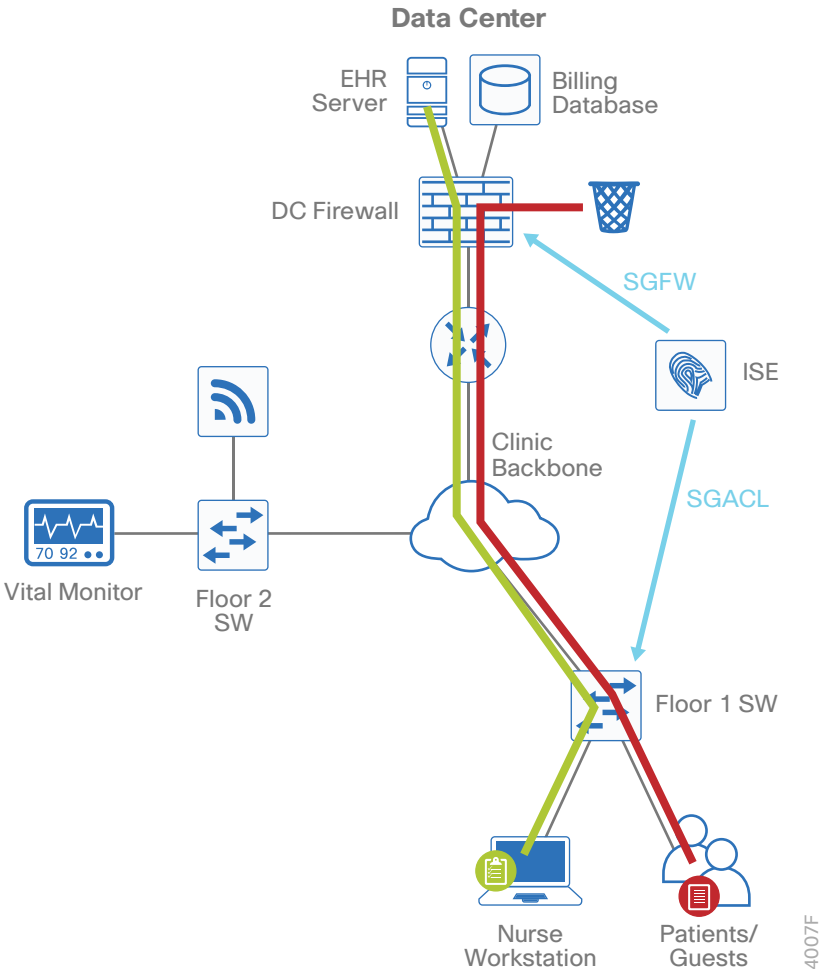


HEALTHCARE: SECURING ACCESS TO MEDICAL DEVICES AND ELECTRONIC HEALTH RECORDS FOR HIPAA COMPLIANCE

Business Problem

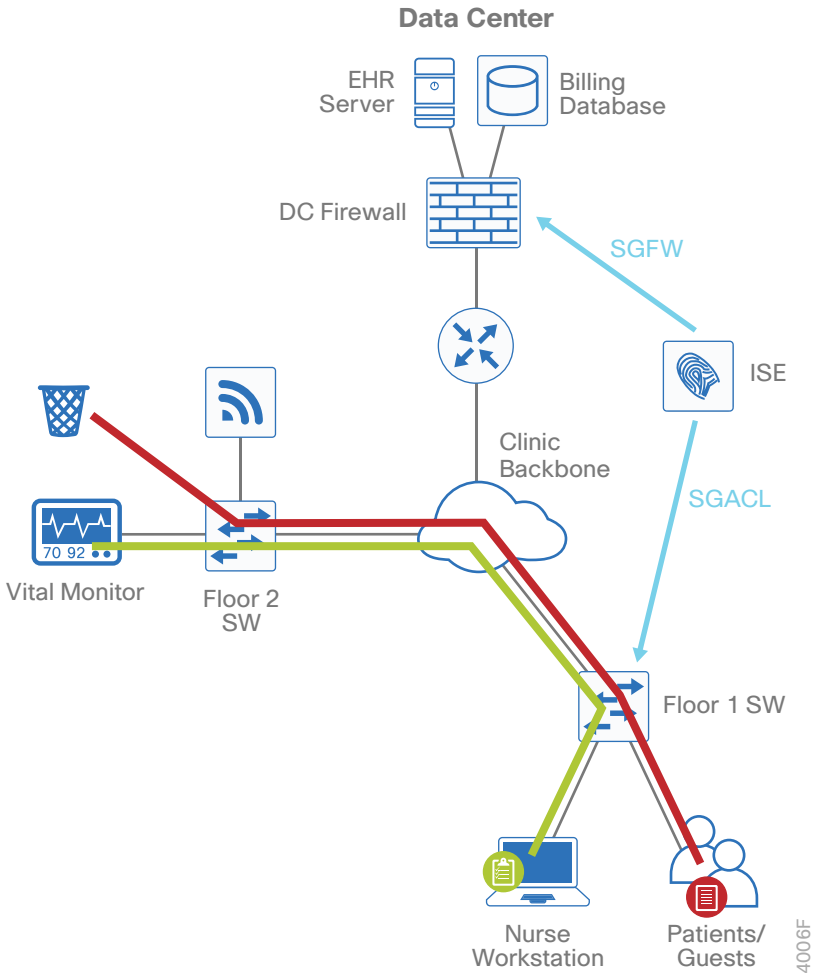
A hospital needs to limit access to electronic health records in order to comply with the Health Insurance Portability and Accountability Act (HIPAA).

Figure 3 *TrustSec for HIPAA compliance*



The hospital also needs to isolate medical devices used for patient care so that only authorized users, devices and servers have access to these medical devices.

Figure 4 *TrustSec for medical device segmentation*



Solution

Medical professionals use an authorized workstation in order to gain access to the electronic health records. The user authenticates to ISE and the device is verified to make sure it is authorized for access to the health records. The switch or WLC tags (with an SGT) the traffic from this workstation. The policy is enforced on the DC firewall with a Cisco Security Group Firewall (SGFW) that allows access to the electronic health records server only to those devices and users that are authorized, and all other devices and users are denied access.

SGTs are applied to authenticated users of medical devices and servers in order to explicitly allow access for authorized users. Devices and users on the network that don't receive the SGT assigned are denied access.

FINANCE: BANK BRANCH NEEDS TO PROVIDE DIFFERENTIATED ACCESS FOR THE VARIOUS SERVICES AT A REMOTE SITE

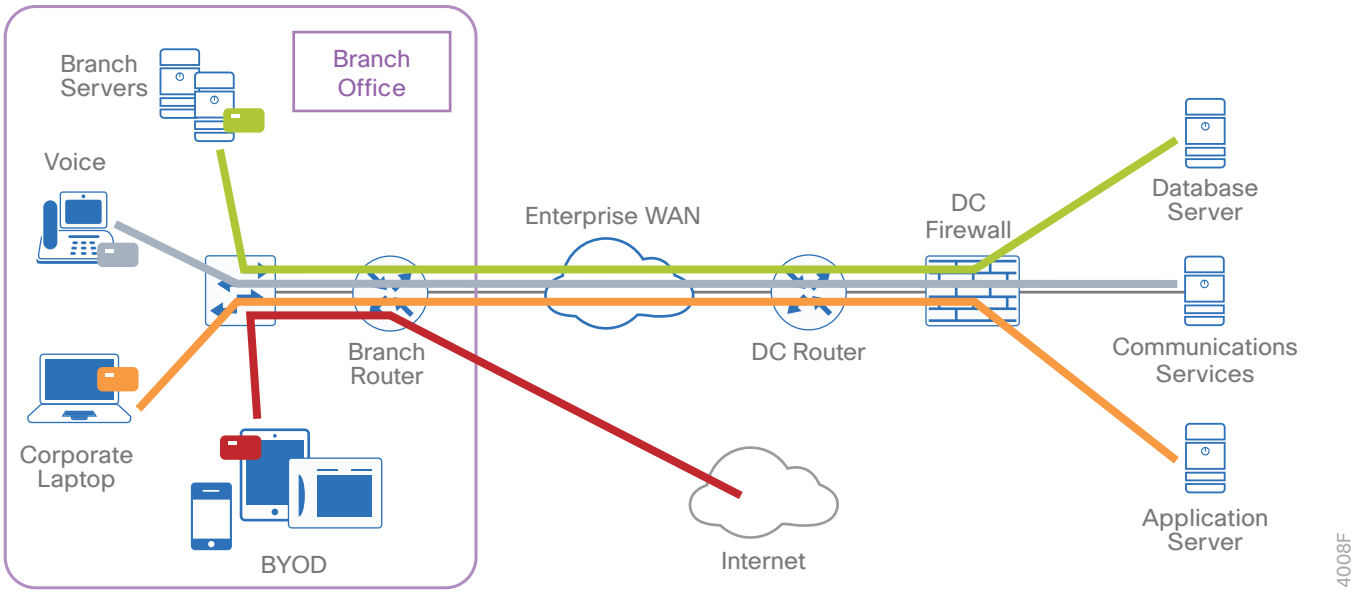
Business Problem

A financial customer requires segmentation of their various services at a remote office. The employee traffic, voice traffic, and server traffic must be in separate networks, as will any guest or bring your own device (BYOD) access. Each individual service must only be given access to the services that are required.

Solution

Each service at the remote site is in its own VLAN. When a device or user accesses the network, ISE authenticates and profiles them. The switch tags the traffic per VLAN, and then the policy is enforced on the remote site router using SGACLs as well as at the DC firewall using SGFW. Corporate traffic is only allowed access to the specific resources required for them. In this case, the employee can access the application server, the phone accesses the communication services, and the remote site server has access only to the database server. The guest or BYOD traffic is given access only to the Internet. With this topology, the VLAN scheme and tagging per VLAN can be replicated at every remote site, making policy configuration simple.

Figure 5 *TrustSec for remote site segmentation*



LINE OF BUSINESS ACCESS CONTROL IN LARGE ENTERPRISES

Business Problem

New business risk and regulatory concerns require the business to implement security controls for users to the data center and within the data center:

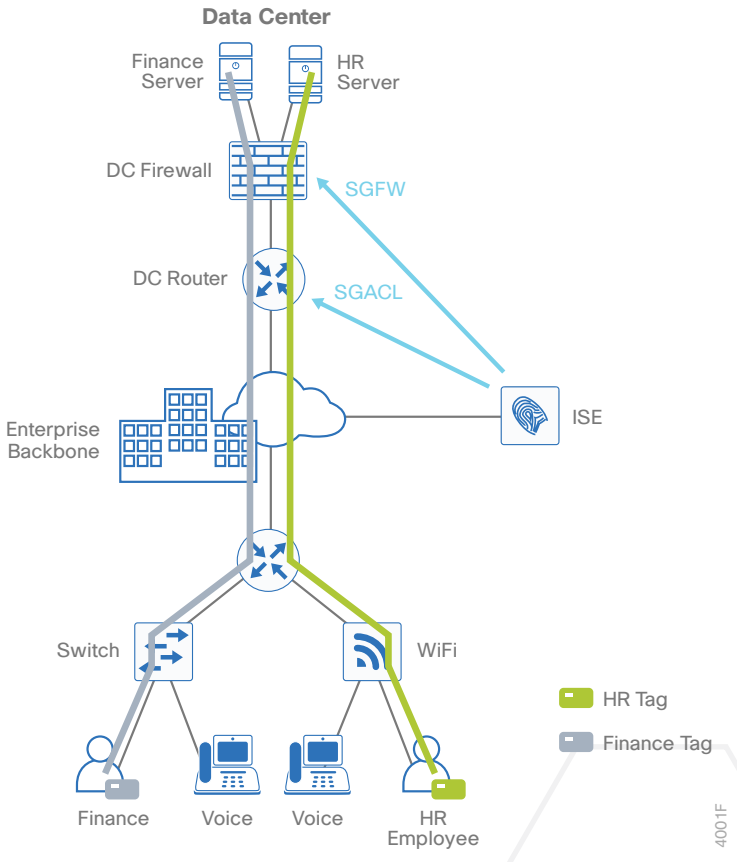
- Users (and devices) should only be allowed to base services and corresponding line of business applications.
- Applications should be segregated by line of business as well as restricted within the line of business.
- Policies are automatically applied for partner/contractors for application and other services.

Solution

Controlling the Services a User Can Access Based on Group Membership

Within the data center, there are specific resources available to different groups of users. For example, there are two servers in the data center, one that only the Finance group can access and another that is only for the Human Resources group. Users identified as members of either group are allowed access to their respective server, and any traffic from any other group is blocked by either the firewall or the data center router.

Figure 6 *TrustSec for line-of-business access control*

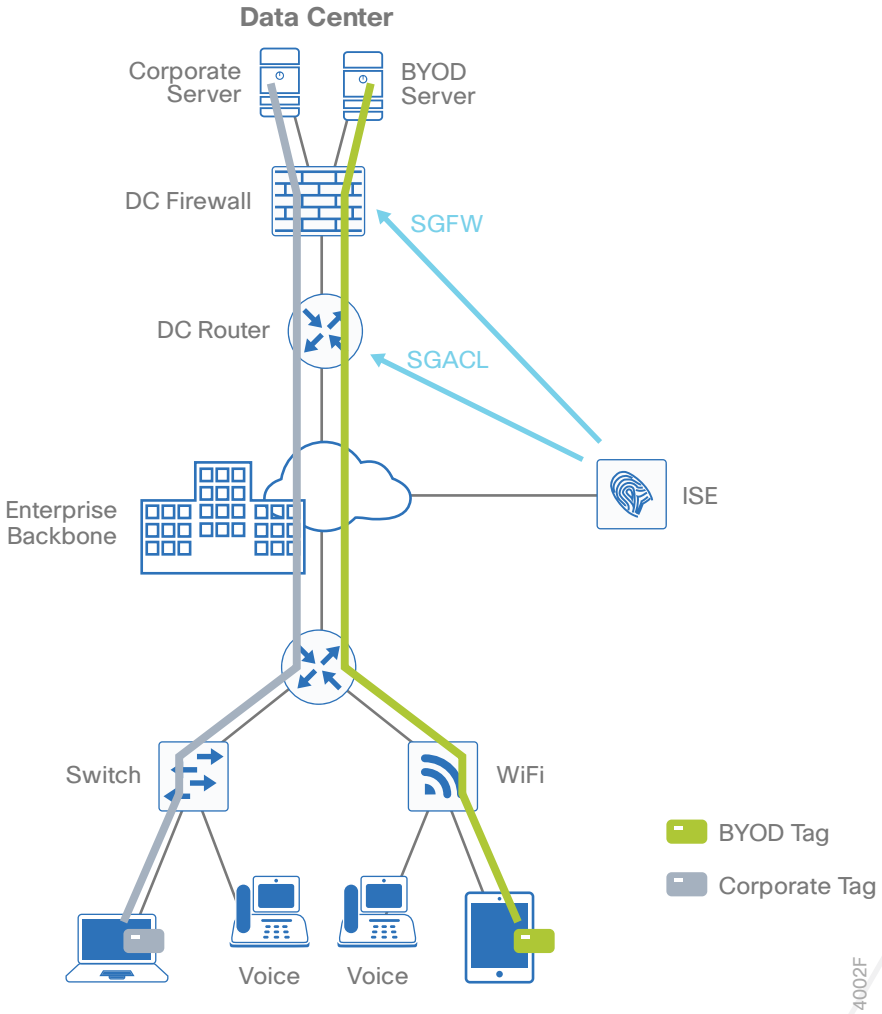


When the user first accesses the network, they authenticate. The switch or the wireless LAN controller (WLC) authenticates the user by using the Cisco Identity Services Engine (ISE), and the user is assigned a tag. The switch or WLC tags (with the SGT) the traffic from this user. The policy is enforced, based on the SGT, in the data center with a security group access control list (SGACL) on the DC router or the with an SGFW on the DC firewall.

Permitting Access to Data Center Resources Based on Device Type

An organization may have a BYOD policy that allows employees to use their smartphones and tablets for work. However, some services may not work well on these platforms, or perhaps policy doesn't allow personal devices access to certain resources. These devices are profiled, classified, and prevented from accessing services not intended for their use.

Figure 7 *TrustSec for BYOD*

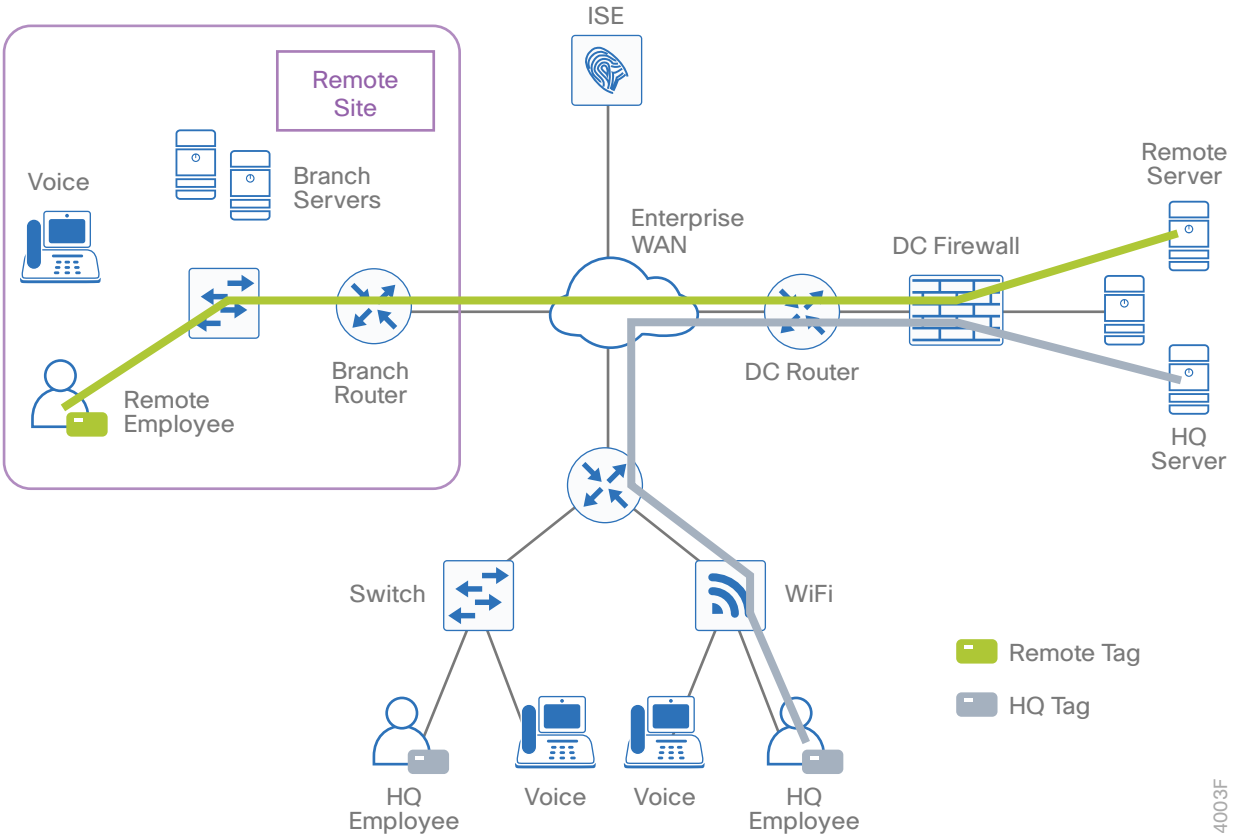


The user accesses the network with their BYOD device and is prompted for authentication credentials. Upon successful authentication, ISE profiles the device in order to determine the type of device, and the user is assigned a tag based on a combination of user and device type. The WLC tags traffic from the BYOD device and the user is limited to the BYOD server in the data center. This is enforced on the DC router with an SGACL or on the DC firewall with an SGFW.

Providing Differentiated Access to Data Center Resources Based on the User and Location

An organization may want to provide different levels of access to services in the data center, depending on where the user is located. There may be a different policy for users at a remote site that limits what the user can access remotely. This policy could also implement different levels of access per remote site or region.

Figure 8 *TrustSec for location-based access control*

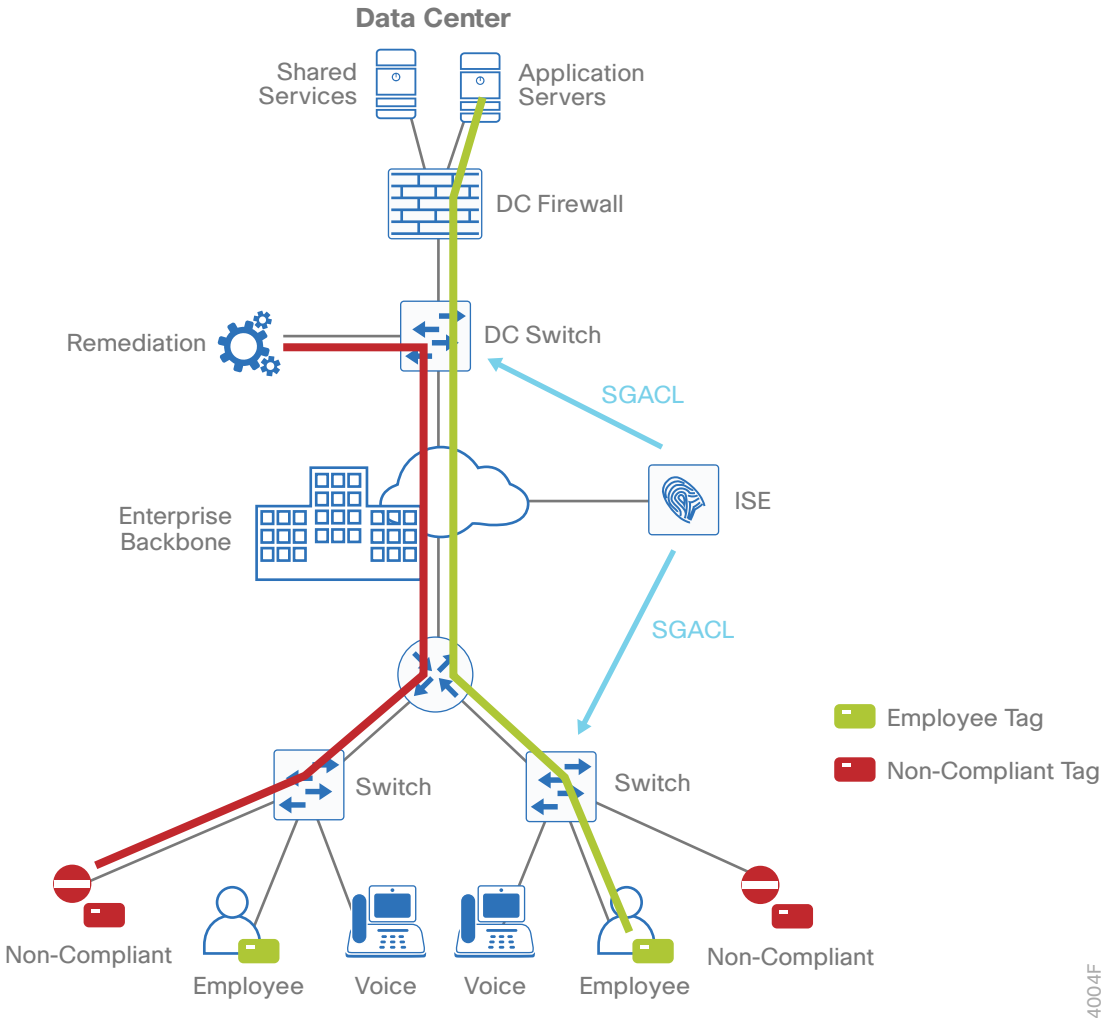


The remote employee accesses the network and authenticates, and the user is assigned a tag. The switch tags this traffic with the SGT, and this tag information is propagated to the DC firewall, where the policy is enforced with an SGFW.

Ensuring That Devices Are Compliant with Security Policy before Accessing Data Center Resources

To comply with security policy, all devices on the network must meet certain requirements, such as running an antivirus application or a minimum version of an OS. Without meeting the policy, the user is denied access to the data center resources and instead given access to remediation services.

Figure 9 *TrustSec for security-policy compliance*



The user accesses the network with a device that does not comply with the security policy. The user authenticates to the network, and ISE profiles the device and checks for compliance. After the device is determined to be non-compliant, the device is assigned a tag that indicates it is out of compliance and limits access to the remediation service. The policy is enforced with an SGACL, at the access switch or at the DC switch.

Next Steps to Ensuring a Successful TrustSec Implementation

1. Based on the use cases outlined above, identify a use case that has realistic criteria for success and has demonstrable return on investment.
   - Model potential group relationships and high-level permissions for the use case.
   - Develop detailed permissions (specific access control lists) off those relationships
2. Apply detailed SGACLs to the use case in a monitoring function in order to detect items outside the security profile.
   - Firewall Access Control Entries (ACE) logging analysis (if available)
   - SGACL ACE logs and syslog analysis
   - ACE log for unknown/SGT or SGT/unknown matches for the use case
   - Default permission of ACE log for anything that "missed" the explicit permission
   - Monitor mode SGACLs, if available (Cisco Catalyst 6500 Series)
3. Gather feedback from the above analysis and iterate with the permissions.
4. Finalize permissions and create completed TrustSec matrix.

Please use the feedback form to send comments and suggestions about this guide.

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.