

Securing BYOD with Cisco TrustSec Security Group Firewalling

Getting Started with TrustSec

What You Will Learn

The bring-your-own-device (BYOD) trend can spur greater enterprise productivity as employees put their own smartphones and tablets to work. But it also brings new challenges to IT, because it's not enough to securely onboard personal devices on the network; businesses need to tightly control the applications and data center resources those devices can access. Cisco TrustSec[®] security group firewalling provides a simple, scalable mechanism to control traffic from personal wireless devices. And you don't need the technology running on every device to make your network more secure.

This paper describes Cisco TrustSec security group firewalling in two parts:

- **Solution overview:** Learn how Cisco TrustSec makes it easy to tightly control access to resources and applications from mobile devices.
- **How to get started:** Use our step-by-step instructions and see what you'll need to implement security group firewalling in your network today.

Solution Overview: Cisco TrustSec Security Group Firewalling

BYOD changes the way employees work and interact with co-workers and helps them be more productive by using the device of their choice. For these reasons, IT departments have been working to accommodate these demands, rebuilding their networks to support thousands of personal devices connecting to their networks. But the introduction of personal devices into the enterprise raises new security concerns. For example, you may allow executives full network access from a wired workstation, but when they connect from a personal device, you want to give them access to corporate email and the intranet while blocking access to critical resources.

Cisco TrustSec gives you a simple, scalable way to bring personal devices onto a wireless network with a high degree of security. The full productivity benefits of a BYOD environment can be realized without compromising or complicating your network security policy. Let's explore what a Cisco TrustSec solution can do for your business and IT environment.

What Are the Goals for Your BYOD Project?

Some enterprises focus on reducing the cost of enabling employee-owned devices and getting users to connect without involving the IT help desk. Others are just trying to keep pace with the thousands of devices coming onto their networks every day. Typically, BYOD projects can be divided into three use cases:

- Enabling employee-owned devices to access limited resources
- Enabling employee-owned devices to access the Internet only
- Enabling employee-owned devices to access all resources

The simplest option is to lock personal devices out of enterprise resources and restrict them to Internet connectivity. But limiting personal devices in this way undermines the basic purpose of the BYOD project. Why bother allowing employees to bring personal devices into the workplace if they can't access the resources they need to be productive?

The ideal solution would allow employees to securely onboard their personal devices, but limit access to specific resources depending on the device and context. But many enterprises find this enormously challenging if they rely on traditional wireless security and network segmentation practices.

Balancing Strong Security with Flexible Access

The industry has a well-defined set of solutions for securing the wireless network, and there are many "best practices" you can follow to tightly control access and traffic from mobile devices on the corporate network. But when trying to implement fine-grained control over the specific resources and applications users can access from a personal device, traditional wireless security designs quickly become unwieldy.

Typically, enterprises use single or multiple Secure Set Identifiers (SSIDs) for the wireless LAN, and users decide which SSID to use depending on the context. For example, employees may use the "Corporate Wi-Fi" SSID, while a separate "Guest Wi-Fi" SSID is available to visitors and guests. In traditional network designs, each SSID is mapped to virtual LAN (VLAN), where users of the same type are put into the same network subnet.

When implementing a BYOD policy, you can create a new dedicated SSID (for example, "BYOD Wi-Fi") or simply reuse the Corporate Wi-Fi SSID and change the VLAN associated with a personal device after authorizing it on the network. In either case, you are creating another VLAN for the BYOD project because these devices need to be treated differently than, for example, a wired corporate workstation. Personal devices are segregated from normal corporate devices because IT doesn't know how secure they are. This is why, in most early BYOD implementations, enterprises provide a BYOD VLAN that limits personal devices to Internet-only access.

Most IT groups trunk VLANs to the core side of the enterprise network and implement security policies at the point in the network where that VLAN links to other network segments. To segment personal devices, some groups use access control lists (ACLs) on network devices (LAN switches or routers, for example), while others use the corporate firewall as a gateway to monitor all traffic coming from the wireless LAN. Typically, those ACLs and firewall rules are maintained manually.

You can therefore understand why so many enterprises provide Internet-only access to personal devices. To provide selective access to corporate services for BYOD users (for instance, allowing BYOD users to access their email, intranet Web servers, and communication tools, but not allowing access to critical assets in the network), you have to define the ACLs and firewall rules associated with all resources you want to enable or protect. In a large enterprise network, this can quickly run to hundreds of thousands of lines of code - an enormous operational headache for IT. And since the network is constantly changing, those ACLs and firewall rules must be actively maintained, which can lead to exploitable human errors.

Simplifying BYOD Access and Policies

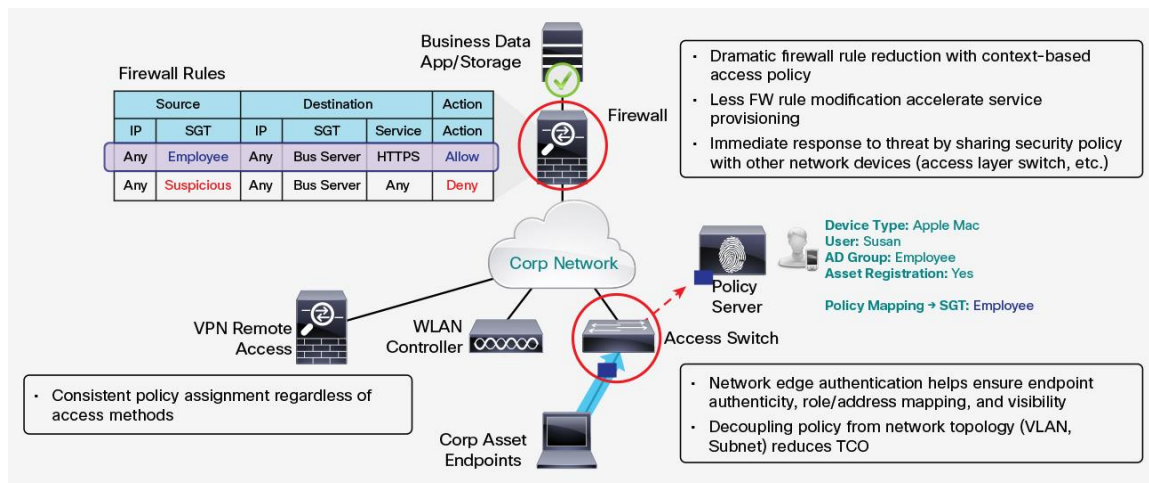
Cisco TrustSec is designed to address both of these pain points: simplifying traditional VLAN-based designs and reducing the operational effort of security maintenance. The basic concept is simple: Instead of managing the network using complex IP addresses (and subnets and VLANs), Cisco TrustSec solutions aggregate BYOD devices or network servers into security groups that are, in comparison, ridiculously easy to manage and ensure your policy is being enforced. Those security groups are tagged with a simple name in plain language that any administrator can understand. Examples could be BYOD-Device, HR-Database, and Mail-Servers. Once you define your security groups, you can then define the policies between them. For example, traffic tagged “BYOD-Device” can communicate with Mail-Servers but not with HR-Servers.

The advantage is that you can assign endpoints and servers to a security group regardless of the logical topology (say, the VLAN or subnet). Even better, you can now manage policy with security group tags instead of IP addresses. So you don't have to keep adding VLANs to your wireless network or maintain thousands of lines of code to parse out the specific IP addresses that different types of traffic can access. Once you define the policy between two security groups, you can keep reusing it for other devices. There is no need to add IP addresses, subnet ranges, or network objects when other resources become available in the corporate network. As long as the traffic or resource has that security group tag, the network knows exactly how to handle it.

BYOD Access in a Wireless Network

Cisco TrustSec technology is supported on both the Cisco® 5508 Wireless Controller and the Cisco 5760 Wireless LAN Controller (WLC). The Cisco WLCs connect both corporate assets and personal devices to the wireless LAN with a high degree of security and assign a security group tag (SGT) based on authentication information. Policy is created and maintained on the Cisco Identity Services Engine (ISE). Once users or devices are classified in a security group, this information is shared between the Cisco WLCs and the corporate firewall device, such as a Cisco ASA 5500 Series Adaptive Security Appliance. On the Cisco ASA, you can simply add firewall rules based on SGTs instead of having to define them based on IP addresses or subnets (Figure 1).

Figure 1. Overview of Cisco TrustSec SGTs



Extending Security Policy to the Wired Network and Remote Access

Cisco TrustSec is supported on more than Cisco WLCs and Cisco ASAs. It is also available on a broad range of Cisco Catalyst® switches. So if you want to extend strong security policy to both wired and wireless devices, you can use the same Cisco TrustSec mechanisms in your wired network, often using the Cisco network devices you already have in place. Cisco TrustSec is supported on the following Cisco Catalyst switches:

- 2960S, 2960-X, and 2960-XR Series
- 3560-X and 3750-X Series
- 3850 Series
- 4500 Series with Supervisor Engine 7-E or 8-E
- 6500 Series and 6880-X

You can also extend Cisco TrustSec policies to employees connecting via remote access. When an employee accesses the enterprise network through an SSL VPN, for example, the Cisco ASA firewall simply assigns an SGT to those VPN users. The result: You gain the ability to apply strong, simple, and consistent security policy to every device connecting to the network, regardless of access method.

In addition, you don't have to use a Cisco ASA firewall to enforce the policy. You can use:

- Many Cisco Catalyst switches
- Most Cisco Nexus® data center switches, including the Cisco Nexus 6000 and 7000 Series and the 5500 and 5600 platform
- Cisco Integrated Services Routers (ISR) G2, including the Cisco 890 and 4451-X ISRs and the 1900, 2900, and 3900 Series
- Cisco ASR 1000 Series Aggregation Services Routers
- All enterprise-level Cisco routers

The result: You have total flexibility to implement security group tagging in your network for all types of access. And you can easily implement selective access to applications and resources for personal devices. So your employees can realize the full productivity benefits of using their devices without compromising corporate security or adding complexity and operational overhead for IT.

How to Start Implementing a BYOD Project

Let's take a closer look at how you would implement Cisco TrustSec security group tagging in a BYOD workplace. Figure 2 provides an example of a high-level Cisco TrustSec design.

Figure 2. Cisco TrustSec High-Level Design

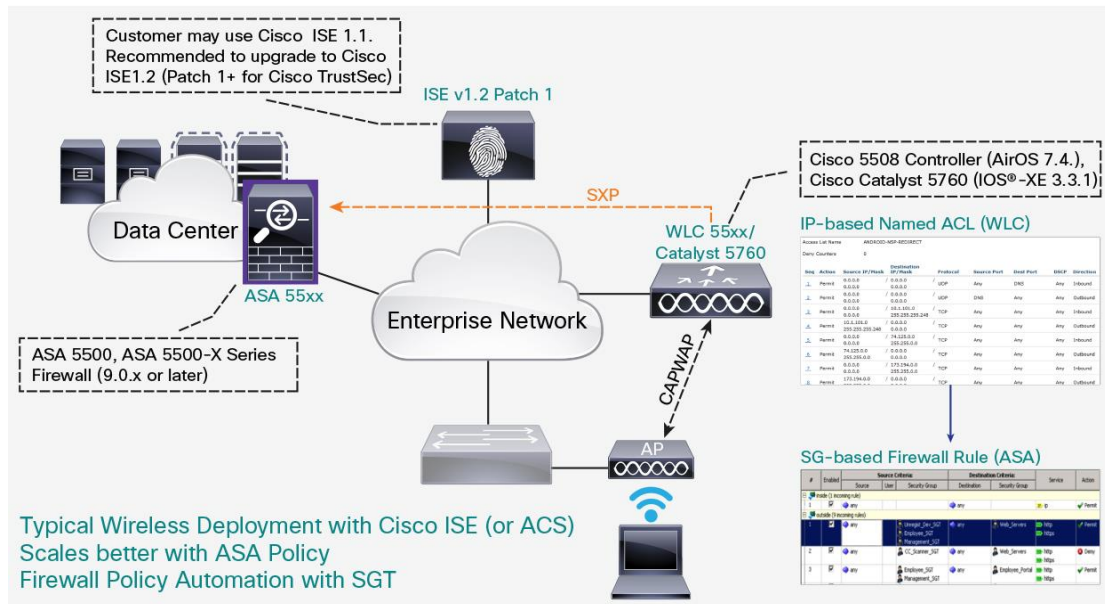


Table 1 provides more details on the components illustrated in this design, and the roles they play in a BYOD implementation.

Table 1. Cisco TrustSec BYOD Components

System Component	Platform	Solution Validated Version	Function
Cisco Identity Services Engine	Cisco ISE 3315, 3355, 3395, 3415, and 3495; appliances and VMware	Cisco ISE 1.2 Patch 5 (requires Advanced license)	Policy server
Cisco Catalyst 2960 Series Switches	Cisco Catalyst 2960-S and 2960-SF Series	Cisco IOS® Software Release 15.0(2)SE2	Campus network access switch
Cisco wireless controllers	Cisco 5508 and 2500 Series; Cisco Wireless Services Module 2 (WiSM2); and Cisco Wireless LAN Controller Module for Integrated Services Routers G2	Cisco AireOS 7.6.100.0	Campus network wireless access controller
	Cisco 5760 Wireless LAN Controller	Cisco IOS XE 3.3.1SE	Campus network wireless access controller
Cisco ASA 5500 and 5500-X Series	Cisco ASA 5505, 5510, 5512-X, 5515-X, 5520, 5525-X, 5540, 5545-X 5550, 5555-X, 5580, 5585-X, and ASA Services Module	ASA 9.2.1, Adaptive Security Device Manager 7.1(5)100, Cisco Security Manager 4.5	Enterprise firewall

Now, let's go step-by-step and illustrate how you implement Cisco TrustSec security group tagging on Cisco ISE, the Cisco ASA firewall, and your Cisco WLC.

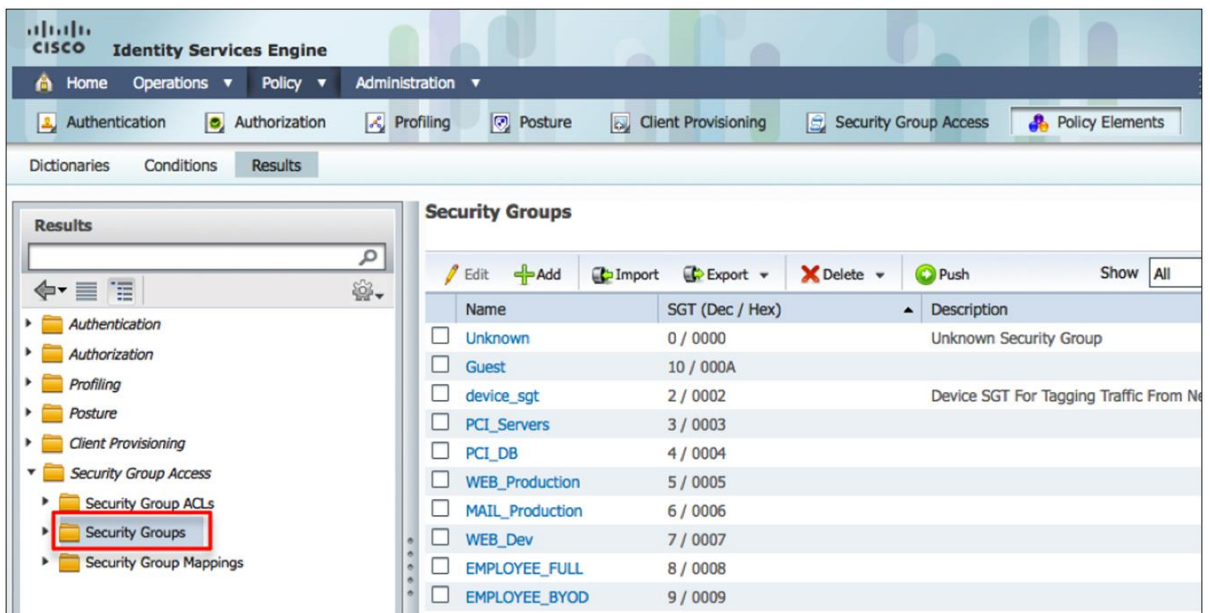
Configuring Cisco TrustSec Tags on Cisco ISE

The first step in implementing a Cisco TrustSec is configuring Cisco ISE. **This example assumes that you have deployed Cisco ISE as your policy engine for wireless traffic and have configured Cisco ISE to support basic wireless 802.1X authentication with a Cisco WLC.** (Note that enabling Cisco TrustSec functions on Cisco ISE requires a specific license.)

To create security group tags on Cisco ISE, follow these steps:

1. Navigate to the Security Group policy menu on Cisco ISE by selecting **Policy > Policy Elements > Results > Security Groups** (Figure 3). The first SGT value you can configure is generated as 2 by default, as SGTs 0 and 1 are reserved.

Figure 3. Defining Security Groups



Name	SGT (Dec / Hex)	Description
<input type="checkbox"/> Unknown	0 / 0000	Unknown Security Group
<input type="checkbox"/> Guest	10 / 000A	
<input type="checkbox"/> device_sgt	2 / 0002	Device SGT For Tagging Traffic From Ne
<input type="checkbox"/> PCI_Servers	3 / 0003	
<input type="checkbox"/> PCI_DB	4 / 0004	
<input type="checkbox"/> WEB_Production	5 / 0005	
<input type="checkbox"/> MAIL_Production	6 / 0006	
<input type="checkbox"/> WEB_Dev	7 / 0007	
<input type="checkbox"/> EMPLOYEE_FULL	8 / 0008	
<input type="checkbox"/> EMPLOYEE_BYOD	9 / 0009	

2. Register the Cisco ASA firewall on Cisco ISE to exchange SGT information between Cisco ISE and the Cisco ASA (Figure 4). Navigate to the Cisco ISE menu **Administration > Network Resources > Network Devices**, and then add the network device entry for the Cisco ASA. Enter the device name and IP address first. Then, select the check box for **Authentication Settings** with **Shared Secret** for the RADIUS protocol.

Figure 4. Adding Cisco ASA

The screenshot shows the configuration page for a Cisco ASA device. The breadcrumb is "Network Devices List > ASA5585-X". The "Network Devices" section includes fields for Name (ASA5585-X), Description, IP Address (10.1.48.2 / 32), Model Name, Software Version, Network Device Group, Device Type (All Device Types), and Location (Data Center). The "Authentication Settings" section is expanded, showing "Enable Authentication Settings" checked, Protocol set to RADIUS, Shared Secret (masked), Enable KeyWrap (unchecked), Key Encryption Key (masked), and Message Authenticator Code Key (masked). Key Input Format is set to ASCII.

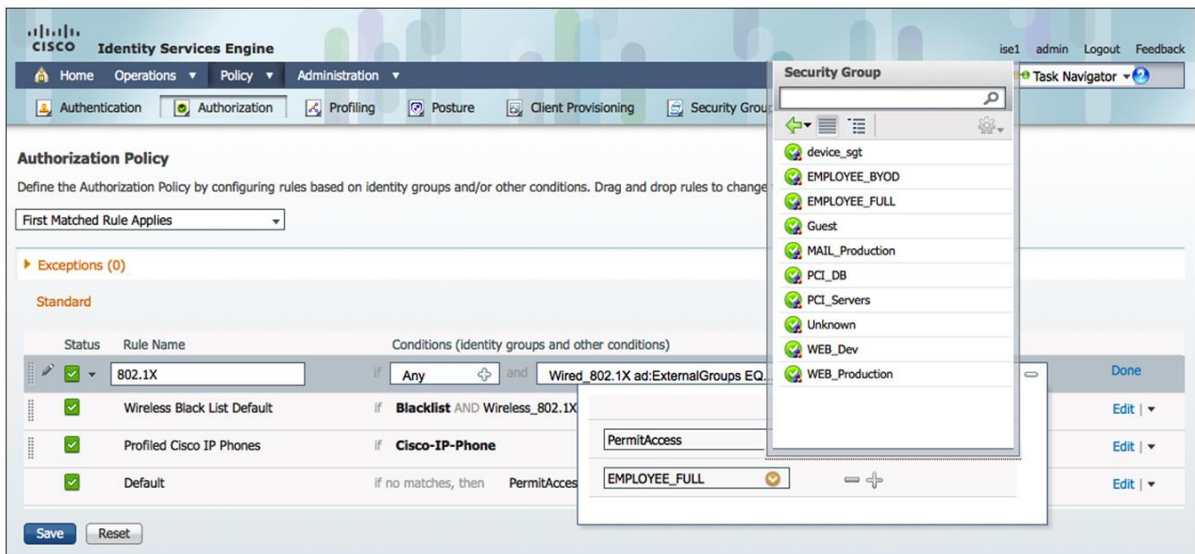
3. On the same Cisco ISE network device page, select **Advanced TrustSec Settings** (Figure 5). Select the check box for **Use Device ID for SGA Identification** and enter the password of your choice. The identical device ID and password are configured on the Cisco ASA as well.

Figure 5. Advanced Settings

The screenshot shows the "Advanced TrustSec Settings" section. Under "Device Authentication Settings", "Use Device ID for SGA Identification" is checked, with Device Id set to ASA5585-X and Password masked. Below are sections for "SGA Notifications and Updates", "Device Configuration Deployment", and "Out Of Band (OOB) SGA PAC". The OOB SGA PAC section shows Issue Date (14 Sep 2013 00:00:24 GMT), Expiration Date (14 Sep 2014 00:00:24 GMT), and Issued By (admin), with a "Generate PAC" button.

4. In the **Advanced TrustSec Settings** window, there is an **Out of Band (OOB) SGA PAC** section. If you click the **Generate PAC** button, a pop-up window appears. Enter **Encryption Key for PAC** (you choose the key) and set the **PAC Time to Live** to **1 year**. PAC is a special security file that the Cisco ASA and Cisco ISE will share to exchange secret information.
5. Create the Network Access Policy associated with the SGT (Figure 6). This part of the configuration is required to assign the SGT to a specific role (users or devices). Navigate to the Cisco ISE menu **Policy > Authorization** and you will see an existing Authorization Policy table for wireless access. Select and double-click the authorization rule that you want to associate with an SGT value. Under the **Permissions** column, click the **+** (plus sign) to add more permissions to the rule. (To add a second permission, click the **+** symbol one more time.) Using the picker, navigate to **Profiles > Security Group** and select the SGT you would like to associate with the rule.

Figure 6. Creating a Network Access Policy



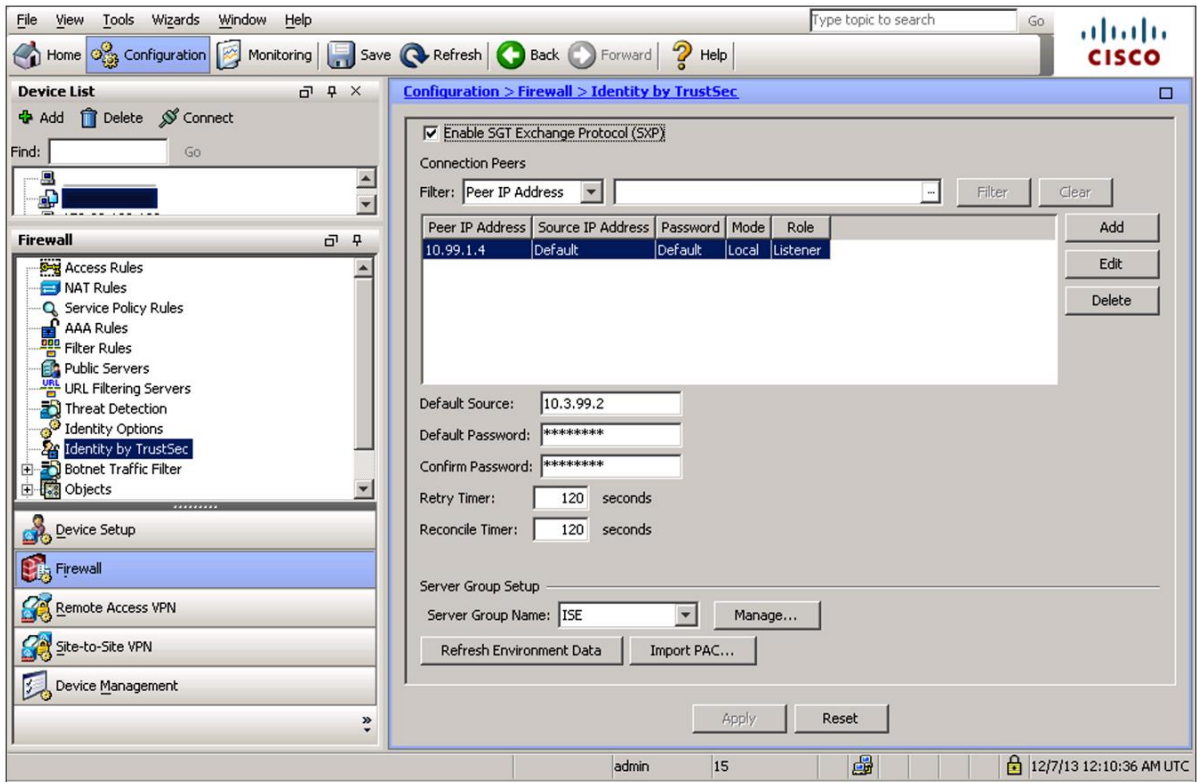
Configuring Cisco TrustSec Tags on a Cisco ASA Firewall

After you modify your Cisco ISE configuration to enable Cisco TrustSec SGTs, the next step is to configure the Cisco ASA. **This illustration assumes you have already configured your Cisco ASA to perform basic firewall filtering.**

Follow these steps to configure the Cisco ASA:

1. First, establish a secure tunnel with Cisco ISE using the PAC file you generated in the previous steps. Navigate to the ASDM tool menu **Configuration > Firewall > Identity by TrustSec**. Note: You will need to create an AAA server entry for Cisco ISE. You can find configuration steps in this [guide](#).
2. After the AAA entry is configured for Cisco ISE, you can import the PAC file you generated in the previous step (Figure 7). Click the **Import PAC** button, click the **Browse** button to browse to your PAC file, enter the **encryption password** you configured on Cisco ISE, and click **Import**.

Figure 7. Importing the PAC File



- Once you have successfully imported the PAC file, the Cisco ASA communicates with Cisco ISE using the RADIUS protocol. You can confirm this communication and shared data by navigating to the ASDM menu **Monitoring > Properties > Identity by TrustSec > PAC**. You can also click **Environment Data** to verify that the Cisco ASA has downloaded SGT and SGT Name Table content from Cisco ISE.
- The final configuration on the Cisco ASA is to configure the SGT Exchange Protocol (SXP) to receive the IP-SGT mapping table from the Cisco WLC. Navigate to the ASDM menu **Configuration > Firewall > Identity by TrustSec** and select the **Enable SGT Exchange Protocol (SXP)** check box. In the **Default Source** field, enter an IP address of a Cisco ASA that is reachable by the Cisco WLC. Enter your SXP **Default Password** that is used for both the Cisco ASA and Cisco WLC. Then click the **Add** button to configure SXP peering with the Cisco WLC. In the **Add Connection Peer** window, enter the **Peer IP Address** (the Cisco WLC IP address), keep the **Password** as **Default**, keep the **Mode** as **Local**, change the **Role** to **Listener**, and click **OK**.
- Now you're ready to start configuring security policy on your ASA firewall. Navigate to the ASDM menu **Configuration > Firewall** and select **Access Rules** (Figure 8). ASA version 9.0 or later gives you the ability to select a security group for both the Source and the Destination Criteria columns. When creating a policy rule, simply select both the source and destination security groups, which is just like selecting network objects. The security group list should be ready for selection.

Figure 8. Configuring a Security Policy

#	Enabled	Source Criteria:		Destination Criteria:		Service	Action	Hits	Logging	Time
		Source	Security Group	Destination	Security Group					
DC-Inside (1 implicit incoming rule)										
1		any		Any less s...		ip	Permit			
management (0 implicit incoming rules)										
outside (4 incoming rules)										
1	<input checked="" type="checkbox"/>	any	Suspicious_Investigate	Server-C Server-D		ip	Deny	0		Alerts
2	<input checked="" type="checkbox"/>	any	Employees	Server-C		ip	Permit	314		
3	<input checked="" type="checkbox"/>	any	Administrators_Group Network_Services	Server-C Server-D		ip	Permit	1154		
4	<input checked="" type="checkbox"/>	any	Production_Servers	Server-C		ip	Permit	0		
Global (1 implicit rule)										
1		any		any		ip	Deny			

Configuring Cisco TrustSec Tags on a Cisco WLC

After implementing Cisco TrustSec tagging on Cisco ISE and your Cisco ASA, the final step is configuring the Cisco WLC. **This section assumes that you have configured your Cisco WLC to support basic wireless 802.1X authentication with Cisco ISE.** If you are already using your Cisco WLC to perform 802.1X configuration with Cisco ISE, only one configuration on the Cisco WLC is needed to implement Cisco TrustSec tagging. Follow these steps:

1. Log in to the Cisco WLC web-based GUI, and navigate to **Security > TrustSec SXP**. In the **SXP Configuration** section, keep the **SXP State** as **Enabled** and enter the **Default Password** (the same password you configured in the Cisco ASA SXP configuration steps described previously).
2. Click the **New** button to create a new SXP peering configuration. In the **Peer IP Address** field, enter the Cisco ASA IP address and click **Apply**.
3. Once the SXP connection is established, you should see the **Connection Status** change from **Off** to **On** (Figure 9).

Figure 9. Configuring the Cisco WLC



Capitalize on BYOD, without the Complexity

The ability to access corporate resources with personal devices yields major dividends in employee productivity and satisfaction. With a Cisco TrustSec solution, you can empower employees to access the corporate applications and resources they need while protecting others, regardless of device or access method. So you can unlock the benefits of a BYOD workplace in your business without compromising security and without the enormous operational effort of trying to adapt traditional network segmentation mechanisms to thousands of new personal devices.

Start capitalizing on the BYOD revolution today. To learn more, visit <http://www.cisco.com/go/TrustSec>, or contact your local Cisco account representative.




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.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)