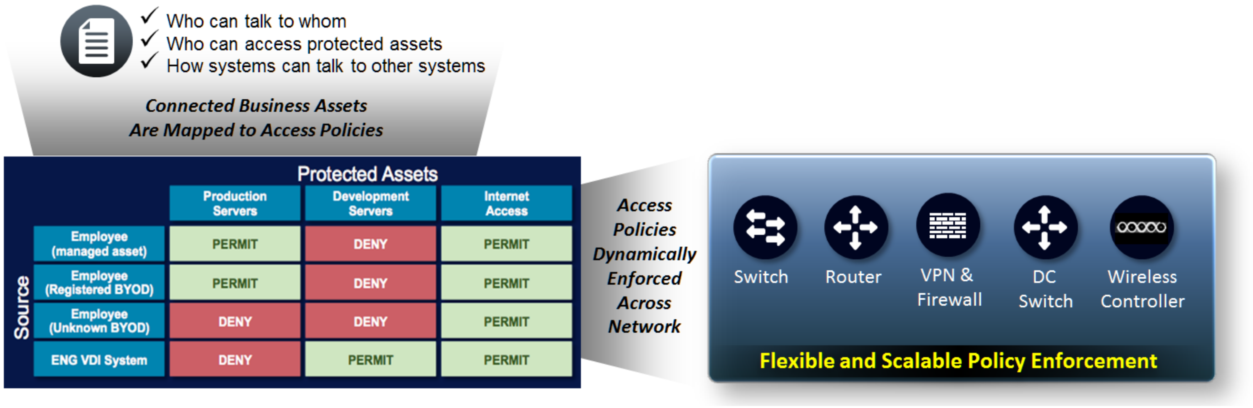
IT-Harvest

Network Segmentation Through Policy Abstraction: How TrustSec Simplifies Segmentation and Improves Security

Sept 2014


✓ Who can talk to whom
✓ Who can access protected assets
✓ How systems can talk to other systems
Connected Business Assets
Are Mapped to Access Policies
Access
Policies
Dynamically
Enforced
Across
Network
Switch
Router
VPN & Firewall
DC Switch
Wireless Controller
Flexible and Scalable Policy Enforcement

Protected Assets

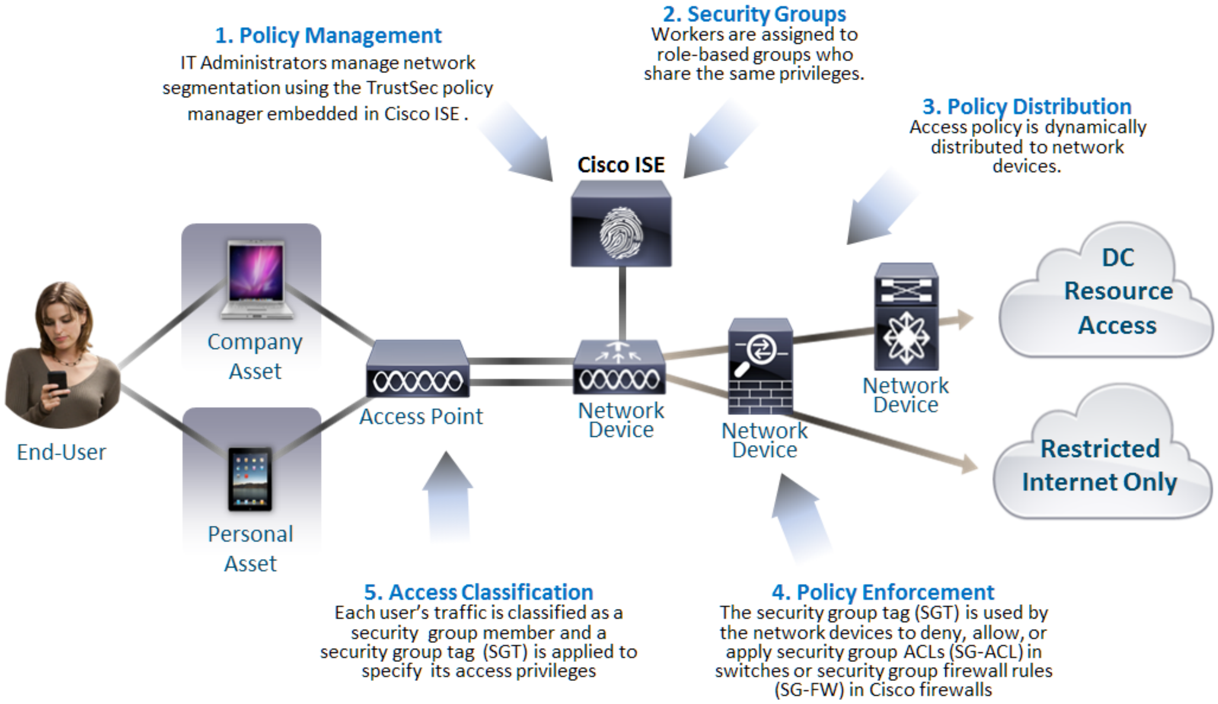
Source	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT

In most organizations networks grow all the time. New stacks of security appliances, new applications hosted on new clusters of servers, new network connections, new subnets, new endpoint platforms and most inexorably, firewall policies and access control lists (ACLs). The natural tendency to deploy network infrastructure in the simplest way possible works during the initial deployment but as each component multiplies, and demands are put on that infrastructure, access control, policy management, and segmenting, become more and more onerous tasks.

By abstracting security policies away from individual components of the network–switches, routers, and firewalls — and centrally locating them — vast improvements in manageability and control are possible. With simplicity comes better security. With a centrally defined network architecture, essentially network segmentation by policy, comes more control, flexibility, and options that can obviate the need for re-architecting physical plant.

How TrustSec Works

Cisco’s TrustSec accomplishes policy abstraction through the logical expedient of assigning roles to devices, users, and network attached resources. When a person or device connects to the network each network component, switch, router or firewall, applies a policy to the network traffic in much the same way a layer 2 switch enforces segmentation via VLANs. Once the traffic is tagged with an identifier each device can enforce a policy based on roles instead of individual IP address or VLAN. Group based policies drastically simplify enforcement as compared to IP-based policies, particularly because IPs change all the time, groups do not. TrustSec also enforces what amounts to layer 3 segmentation, defined centrally.



1. Policy Management
IT Administrators manage network segmentation using the TrustSec policy manager embedded in Cisco ISE .

2. Security Groups
Workers are assigned to role-based groups who share the same privileges.

3. Policy Distribution
Access policy is dynamically distributed to network devices.

4. Policy Enforcement
The security group tag (SGT) is used by the network devices to deny, allow, or apply security group ACLs (SG-ACL) in switches or security group firewall rules (SG-FW) in Cisco firewalls

5. Access Classification
Each user's traffic is classified as a security group member and a security group tag (SGT) is applied to specify its access privileges

Those centrally defined roles also serve to replace the traditional function of switches in controlling network segmentation. Many organizations that have grown quickly or have legacy infrastructure have run out of possible VLAN capacity in their switches. VLANs have always been defined on each switch to create virtual segmentation between departments, data centers, and functional components of a network.

For more mature environments, additional segmentation using more VLANs can outstrip the capability of the IT team to manage it. As an example, when implementing a new segmentation policy, carving out a new VLAN across a global infrastructure is quite challenging to execute without a network redesign or architecture changes.

Traditional internal controls are limited in their ability to answer the questions: who are you, where are you coming from, where are you going? These questions are answered based on network topology. An employee coming in over a VPN was granted access based on their permissions. The ACLs in switches and routers needed to enforce those policies could quickly grow beyond their capacity to enforce them at line speeds and any changes to network topology or access policies created a management nightmare. Essentially, ACL-based enforcement is typically 'ingress' ACLs, which means that the ingress enforcement device needs to understand the universe behind it (down to the IP addresses or IP subnets that it needs to protect). So if any new resource is added, all the ingress ACLs, across all the ingress access switching infrastructure needs to be updated

SGTs and SG-ACLs

Most Cisco devices are already configured to accommodate TrustSec and that list is growing.[1] Cisco has defined Security Group Tags (SGTs) that are distributed to network infrastructure based on enforceable group polices. Once users/devices are authenticated to the network using Cisco Identity Services Engine (ISE) — be it a laptop, desktop, server, printer, even smoke alarms and video cameras, and other things — it is connected and assigned its proper role with an appropriate SGT, it can only connect to approved servers with approved protocols, enforced by Security Group ACLs (SG-ACLs) in network devices.

Each network device automatically downloads SG-ACLs from Cisco ISE. An update to SG-ACLs made with Cisco ISE is immediately deployed and enforced across the network. With TrustSec, network-wide changes in segmentation could be accomplished without any changes in network design.

ISE

The Cisco Identity Services Engine[2] is the evolution of Cisco's previous NAC and ACS products. It is available in a physical or virtual appliance form factor. It comes with existing device identifiers that can help assign policies based on manufacturer, model, and configuration. To accommodate the rapid introduction of new devices that is the bane of IT departments everywhere ISE can be configured to download a feed of new device identifiers as they are introduced by manufacturers. Imagine having a policy ready to go for the next Google or Apple products before a power user attempts to connect it to your network! ISE provides the context and device aware policy management function in generating the TrustSec SGTs and SG-ACLs used for segmentation and enforcement in TrustSec enabled network and security devices.

ISE provides policy and access enforcement for allowing someone onto the network. TrustSec provides packet level enforcement across the extended network once someone is authenticated and allowed in (whether via wired, wireless or a VPN.)

Role Management

TrustSec's leap of innovation is the shift from purely network factors (source, destination, protocol) to role and device based access. Using Cisco ISE, a user can define the right SG-ACLs through a simple matrix of roles for users, devices, and servers, ISE that pushes the SG-ACLs to all enforcement points that are TrustSec enabled. Firewalls configured to accept the same Groups can enforce policies even when resources are moved from one subnet to another.

Virtualization

The value proposition for virtualized computing and storage environments has always included flexibility and extensibility, often called elasticity. Compute and storage resources can be spun up on demand and/or moved to where they are needed, from test to stage to production for instance. With TrustSec each service's role can be assigned and each network device can enforce its policy. The savings in management and time can easily be understood.

BYOD

By far the driver for Network Access Control has been the proliferation of mobile devices that need to access network resources, either over VPN or on-campus wireless devices. Enrolling devices, setting policies, and tracking activity is greatly simplified with TrustSec. ISE is integrated with best of breed Mobile Device Management (MDM) solutions and communicates events to leading Security Information and Event Management (SIEM) solutions.

Legacy NAC solutions have been limited to a simple yes-no-maybe policy based on device, location and user. Once a device and user are authenticated they are granted access to the network. Unauthorized users/devices are blocked, and guest users are allowed limited access, usually just to the Internet, sometimes to a single server that may, for instance, provide a retail store directory.

DevOps

This simplification of policy by moving to a higher layer of abstraction will show the most benefit in future deployments of services. Development teams have never been good at defining what security controls will be necessary as a new project is moved into production. Test and development environments are usually topologically flat and most ACLs are set to Any-Any-Any (Any source IP address, over Any port, to Any destination IP address.) It has always been up to the network security team within operations to devise those policies and move them through a burdensome change control process to implement. The security team is put in the position of delaying deployments of business critical apps, usually because sufficient time was not allotted for their tasks.

With role based policies a development effort can be tasked with defining those roles which can be created and even pushed out from ISE well before project completion. For once, security operations and development will be working together to ensure on-time delivery of new projects.

Extended Quarantining

Network access quarantining was the original driver for NAC. The use case was to shunt a new connection to a server that could perform various hygiene tests and provide updates to security software on a laptop or other mobile device. TrustSec takes that further. First by making the location of the quarantine network immaterial. VLANs don't need to be strut together or over complicated in order to quarantine devices connecting anywhere to the network (each physical access switch or WLAN access point.)

But the concept of quarantine is extended by the deep segmentation empowered by TrustSec. A malware infection that gets into a guest network will never have the ability to escalate privileges to get to the finance department. Or an attacker who gets access to an internet facing SQL server will not be able to burrow deeper into the organization.

Internal Resilience

While TrustSec simplifies security operations it will also contribute to better overall security. Recent years have seen the rise of well funded, sophisticated and dedicated attackers. These can include teams that have been tasked by nation states or cyber criminal organizations with particular targets and assets for acquisition. Most such attacks have been shown to seek access via privileged accounts, either of domain administrators, developers, or perhaps executives.[3] Traditional access controls are no defense against such attacks because the enforcement points are at the perimeter. Once an outside attacker gains the privileges of an insider, or for that matter a malicious insider abuses their privileges, they have free reign to search, steal, or destroy their targets.

TrustSec is an important move to a hardened internal defense. Role based policies can be very specific and because they are easy to devise and simple to maintain they can be much more granular than ever before possible. TrustSec provides the path to internal hardening that will serve to reduce the number of impactful breach events and protect an organization's key assets.

TRUSTSEC CASE STUDY

Erickson Living
Hans Keller
Vice President, IT Operations

Hans Keller VP, IT Operations, at Erickson Living, a multi-state assisted living community builder had a unique network and security need. The organization over all provides living accommodations for 23,000 residents in 17 communities spread across ten states and employs a staff of 13,000. There are 5,200 laptops and nurses stations abiding by regulatory requirements of a clinical setting.

The Problem: How to provide internet services over WiFi that was flexible yet secure. After much research Keller created an architecture based on Cisco gear, with TrustSec and ISE being primary contributors to its success. The first community where he rolled out the TrustSec solution had 1,500 homes. Each home needed its own wireless LAN. Residents and their guests, usually their adult children, needed internet access while in the residence and in the common areas.

Each resident has a username/password in Active Directory, which integrates with ISE. Each connection has a security group tag associated with the residence that allows them to access their devices such as NAS, printers and the internet. They can never even see the other WLANs or any other Whiffy devices.

There are a total of seven VLANs in the community, four for administration, and three for each of 500 WLANs. Cisco optical networking devices provide the transport. The community data center hosts an ISE cluster and VMs configured with Active Directory and DHCP.

Erickson Living has solved a complicated network architecture with a simple to deploy and configure solution. End users have minimal support issues. Security is maintained throughout the complex with simple group tags in TrustSec. This example of enabling a network architecture with a security capability demonstrates the power of ISE and TrustSec.

NOTES

1. Cisco TrustSec for Policy-Defined Segmentation http://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/trustsec/at_a_glance_c45-653057.pdf
2. Cisco Identity Services Engine (ISE) At a Glance http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-654884.pdf
3. The RSA Hack: How They Did It http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/