Cisco TrustSec & Identity Services Engine:
Securely Enabling Your Business with Policy based access control

Atif Azim
Product Marketing Manager

Dec 2011

Cisco Confidential
Agenda

• Industry Transformations and Business Drivers
• Introduction to Cisco TrustSec
• The Cisco TrustSec Advantage
• High Level Design Overview
• Deployment Best Practices
• Call to Action
How do I control who and what access the network?
Our Users Have New Expectations
The Evolving Workplace Landscape

OLD SCHOOL

- Enterprise provided mobile devices
- Work is a *place you go to*—limited off campus access
- IT visibility and control into user devices and applications

NEW SCHOOL

- Anywhere, anytime, any device usage
- Work is a *function*—globally dispersed, mixed device ownership
- Change in IT control and management paradigm—granularity beyond device
The Challenge with Access Control

BUSINESS IMPERATIVES

“I need to onboard consumerized IT devices to enable new services”

“I need to enable a productive global and mobile workforce”

“We must be compliant with regulations and able to show it”

SECURITY IMPERATIVES

“Can I Manage the Risks of BYOD”

“Who and what is on my network?”

“I need to segment network and DC assets to limit the scope of compliance”
The Burden Falls on IT

**Compliance Ops**
- How do I ensure compliance with SOX, HIPAA, etc?
- How do I monitor real time usage for full accountability

**Security Ops**
- How do I secure my data as it moves to the cloud?
- How do I secure my virtual desktops?
- How do I implement multiple security policies per user, device?

**Applications Team**
- How do I ensure consistent experience on all devices?
- How to troubleshoot App vs Network vs Device issues?
- How do we ensure Application interoperability?

**Network Ops**
- What devices are on my networks?
- Which users are using what devices?
- How do I support guests on my network?

**Network Engineer**
- How do I troubleshoot Access problems?
- How do I separate device issues from network and policy issues?
- How do I ensure user experience?

**Endpoint Team**
- How and what do I support?
- How do I ensure my endpoints are compliant?
The Ultimate Access Control Solution

INTELLIGENT
Comprehensive Contextual Awareness of the Who, What, Where, When, How

EFFICIENT
Centralized Secure Access Services and Scalable Enforcement Complimenting Your Network

SECURE
Secures access to your critical resources, mitigating risk and ensuring compliance

Lower Total Cost of Ownership
Introducing Cisco TrustSec
Securely Enables Your Business with Policy based access control

- Comprehensive Visibility
- Exceptional Control
- Effective Management
Cisco TrustSec Architecture
Identity and Context Centric Security

- Identity
- User and Devices
- WHAT
- WHERE
- WHEN
- HOW

Centralized Policy Engine
Business-Relevant Policies
Dynamic Policy & Enforcement
Security Policy Enforcement
Application Controls
Monitoring and Reporting
Cisco TrustSec Solution Portfolio

Policy Administration
- Policy Decision

Identity Services Engine (ISE)
Identity Access Policy System

Policy Enforcement

Cisco 2900/3560/3700/4500/6500 and Nexus 7000 switches, Wireless and Routing Infrastructure

Cisco ASA, ISR, ASR 1000

TrustSec Powered

Policy Information

NAC Agent
- No-Cost Persistent and Temporal Clients for Posture, and Remediation

Web Agent
- "802.1x Supplicant"
  - AnyConnect or OS-Embedded Supplicant

Identity-Based Access Is a Feature of the Network Spanning Wired, Wireless, and VPN
Comprehensive Visibility
Identity and Context Awareness

- Guest Access
- Profiling
- Posture

Context

Identity

Identity and Context Aware Information

- Security Camera G/W Agentless Asset Chicago Branch
- Personal iPad Employee Owned Wireless HQ
- Francois Didier Consultant HQ—Strategy Remote Access 6 p.m.
- Vicky Sanchez Employee, Marketing Wireline 3 p.m.
- Frank Lee Guest Wireless 9 a.m.

Cisco Switches, Routers, Wireless Access Points

Identity (802.1X)-Enabled Network
Identity Awareness
Leveraging your Infrastructure Network

Flexible Authentication
- Multiple methods
- Configurable order and priority of methods
- Monitor Mode

Authentication Methods

IEEE 802.1x
- Standard for link layer authentication and access control
- Components: supplicant (client), authenticator (switch), and AAA server
- Uses Extensible Authentication Protocol (EAP) to transport authentication info.

MAC Auth Bypass
- Authenticate using the client’s MAC address
- For devices that don’t support 802.1X (no supplicant), such as printers.

Web Authentication
- For clients that don’t support 802.1X (no supplicant), but are capable for interactive HTTP authentication

802.1X
Authorized Users
IP Phones
MAB and Profiling
Network Device
Web Auth
Guests
Cisco Catalyst Switch
Context Awareness: Device Profiling
Automated Device Classification using Cisco Infrastructure

Device Classification
Profiling for both wired and wireless devices

Deployment Scenario with Cisco Device Profiling

Collection — Switch collects device related data and sends report to ISE

Classification — ISE classifies device, collects flow information and provides device usage report

Authorization — ISE executes policy based on user and device

Efficient Device Classification Leveraging Infrastructure

Comprehensive Visibility
Context Awareness: Posture Assessment
ISE Posture Ensures Endpoint Health before Network Access

Sample Employee Policy:

- Microsoft patches updated
- McAfee AV installed, running, and current
- Corp asset checks
- Enterprise application running

Temporary Limited Network Access Until Remediation Is Complete
Context Awareness: Guest Management
ISE Guest Service for managing guests

Guest Policy:
• Wireless or wired access
• Internet-only access

Provision: Guest Accounts via Sponsor Portal
Manage: Sponsor Privileges, Guest Accounts and Policies, Guest Portal
Notify: Guests of Account Details by Print, Email, or SMS
Report: On All Aspects of Guest Accounts
Exceptional Control
Delivers Policy-based Enforcement

Policy-Based Access Control

Scalable Enforcement
- VLANs
- Access Control Lists
- Secure Group Tags
- MACSec Encryption

Data Center
Intranet
Internet
Security Zones
TrustSec Authorization and Enforcement

Flexible Enforcement Mechanisms in your infrastructure
Range of options available to customer
Policy Enforcement Through the Network

Source Group Access

 Employee

 Partner

 Guest

The Solution

Scalable Enforcement independent of network topology

Group users independent of IP address and location

Packets are tagged based on context (i.e. location, posture, device, user)

Tag assigned at first network egress point

Scalable and simplified management with a single policy per group
MACSec Encryption
Data Protection with Policy-Based Encrypted Access

The Solution
Data Confidentiality with Visibility

Typical Deployment Scenario

- Hop by Hop L2 encryption
- Visibility into the flows for Security and QoS policy enforcement
- Security Group Tag integrity

Flow visible for policy enforcement

Cipher Data
- 802.1 AE Encrypted

Decipher On Ingress Interface

Corporation Resources
Effective Management
Unified (Wired, Wireless, Policy) Management

- Converged Security and Policy Monitoring
  - Contextual status and monitoring dashboards
- Centrally organizes Day 1-to-n management tasks
  - Instructional configuration workflows
- Reduces the time to troubleshoot
  - Integration with Cisco NCS Prime
TrustSec Packaging and Licensing

New TrustSec Features in Existing Switch Packaging:
- Campus (Cat 3K/4K):
  - LAN Base – 802.1X, SXP, IOS sensor, MACSec
  - IP Base – SGT, SGACL
- Aggregation (Cat 6K):
  - IP Base – 802.1X, SXP, SGT, SGACL
- Router (ASR 1K/ISR):
  - Base packaging – SXP
  - Advanced/Security – SG FW
- Data Center (Nexus):
  - Advanced LAN License → Base Package

Appliance Platforms
- Small 3315/1121 | Medium 3355 | Large 3395 | Virtual Appliance

Note: Advanced License does not include Base
**TrustSec Advantages:**
Different from Competitors

- One Policy for Wired, Wireless and VPN
- Integrated Lifecycle Services (Posture, Profiling, Guest)
- Differentiated Identity Features (Multiple Auth Methods, Flexible Sequencing Auth)
- Phased Approach to Deployments—i.e. Monitor Mode
- Flexible and Scalable Authorization Options
- Encryption to Protect Communications and SGT Tags
TrustSec Deployment
ISE Nodes and Personas

Persona – One or more of the following:
- Administration
- Monitoring
- Policy Service

ISE

OR

ISE

Single ISE Node
(appliance or VM)

Single Inline Posture Node
(appliance only)
Centralized Deployment

All ISE Persona’s deployed in a single site

Distributed Deployment

ISE Persona’s deployed across multiple sites
Deployment Overview

1. Planning
2. Proof of Concept
3. Pilot Deployment
   - No Enforcement (Monitor Mode)
   - Enforcement (Low Impact Mode)
   - Supplicant Provisioning
   - RADIUS Setup
   - Switch Setup

**Typical TrustSec deployment Scenario**
- Plan in advance and keep user experience impact as minimum as possible

(Size: 1 segment or 1 floor)

 Expansion

(Size: Multi-Floor, Bldg.)

Services

Review & Adjust

Review & Adjust
Getting Ready for Your Deployment

“Project starts with Network / Infra team. Later on, security team is involved. And at last we realized we needed to talk with Desktop team in first place…”

Deployment Planning

TrustSec Project involves Network Team, Security Team, and Desktop Team

Planning Phase Discussions:

- What to manage (Managed/Unmanaged Device)
- Policy Definition: Security Level, Trade-offs
- HA design, Disaster Recovery Plan
- Phase Goal, Max Endpoint
- Device Type, OS Type, Supplicant Type, Authentication Methods, current credential store Type (backend DB type)

Sample Questionnaire

Project Overview and Organizational Ownership

OS Type, Supplicant Choice, Auth Type and other application restriction

Network Device

AAA Infrastructure

Current directory service

Service Requirement
Secure Access to Your Network Now!

“Visibility and Control”

“ISE Advanced + Base” Offer

“BYOD—Bring Your Own Device”

“ISE Wireless” Offer, Expand to Wired

“Secure Data Center”

Identity/SGA + ISE Advanced

TrustSec™—Securely Enables Your Business with Policy based access control
Thank you.
Cisco SecureX Architecture

Threat Intelligence (SIO)

Context Aware Policy

Context Aware Enforcement
Integrated | Overlay | Cloud

Network
Visibility | Context | Control

Application Programming Interfaces

Management Services Partners

Cisco Secure Intelligence Operations (SIO)

Secure Endpoint

Cisco Infrastructure Control

Visibility

Cloud

Management

Services

Partners

Secure Virtual and Cloud

AnyConnect

Nexus 1K and Cloud Connected Network

Cisco Secure Intelligence Operations (SIO)