Cisco Secure Access Control

Delivering Deeper Visibility, Centralized Control and Superior Protection

Marko Tanaskovic, CSE, GSSO
Christian Schulmeister, CSE, GSSO
June 2016
1. Cisco Security Vision
2. Access Control with ISE
3. ISE 2.1 and Anyconnect 4.3 - NEW
4. ISE 2.1 GUI Demo
It’s Harder Than Ever to See Who Is on Your Network and What They Are Doing

90% of surveyed organizations are not “fully aware” of the devices accessing their network

75% of companies say their mobile devices were targeted by malware in the last 12 months
Today’s Networks Require Better Visibility and Stronger Control

Key trends creating weaknesses in legacy networks

- Mobility and BYOD in the workplace
- Digitization of data
- Internet of Things (IoT) connecting everything
While Protecting an Ever-Increasing Amount of Data

300% Average enterprise network data growth over the next 5 years¹

See and Share Rich User and Device Details

- **Gain consistent cross-platform user and device visibility and control**
- **Improve your existing security and network solutions**
- **Make network events actionable**

See who and what is on your network and share across network solutions.
Stop and Contain Threats

Reduce risk and contain threats by dynamically controlling network access

Ease security policy setting

Limit unnecessary network exposure

Prevent threats from compromising your network in real time
SECURITY EVERYWHERE

Attack Continuum

Before  During  After

Endpoint  Branch  Edge  Campus  Data Center  Cloud  Operational Technology

Services
Better Security Visibility

Securing the Mobile Enterprise

Protect Against Advanced Malware

Improve Results with Security Services

Harden and Segment the Network

Security as a Network Driver
Our goal is to make security less complex by providing a best of breed portfolio that’s deeply integrated and delivers solutions that are superb individually, but vastly more powerful when used together.

Know your enemy and know yourself and you can fight a hundred battles without disaster.

Sun Tzu
Introducing
Identity Services Engine 2.1
Introducing Cisco Identity Services Engine (ISE)

A centralized security solution that automates context-aware access to network resources and shares contextual data.

- Identity Profiling and Posture
  - Threat (New!)
  - Vulnerability (New!)
  - Who
  - What
  - When
  - Where
  - How
  - Compliant

- Access Policy
  - Traditional
  - Cisco TrustSec®

- Network Resources
  - Guest Access
  - BYOD Access
  - Role-Based Access
  - Threat Containment

- Network Door
  - Physical or VM

- pxGrid Controller

- Context
Context Enhances Protection Across the Attack Continuum

- Gain visibility into who and what is on your network
- Grant access on a “need to know” basis

- Provide threat context to network behavioral analysis
- Contain through network elements and security ecosystem

- Get better forensics and prepare for the next attack by sharing information with ecosystem partners
Cisco ISE – Features and Licensing

**AnyConnect Apex** (Term License)
- Unified Posture Agent
- All AnyConnect services including Network Visibility Module

**Apex** (Term License)
- Endpoint compliance and remediation
- MDM/EMM capabilities
- AnyConnect Unified Agent Services*
  *Requires AnyConnect Apex licenses

**Plus** (Term License)
- Device profiling and feed service
- BYOD with certificate authority
- Cisco® pxGrid context sharing
- Adaptive Network Control

**Device Admin** (Perpetual License)
- TACACS+

**Base** (Perpetual License)
- Guest services
- Cisco TrustSec
- AAA
- RADIUS/802.1X

*Requires AnyConnect Apex licenses*
What Is New?
What Is New in ISE 2.1 and AnyConnect 4.3

- Threat-Centric NAC
- AnyConnect® NVM Enhancements in Version 4.3
- ISE Technology Partner and pxGrid Enhancements
- Context Directory
- ACS to ISE Migration
- Easy Connect
- Streamlined Visibility Wizard
- Cisco TrustSec® and Cisco ACI™ Policy Plane Integration
- Dashboard Enhancements
- Rapid Threat Containment (RTC)
AnyConnect 4.3
AnyConnect – Way more than VPN

AnyConnect features

- Basic VPN
- Advanced VPN
- Endpoint Compliance
- Inspection Service
- Enterprise Access
- Threat Protection
- Network Visibility

Integration with other Cisco solutions

- ISR
- ASR / CSR
- Adaptive Security Appliance (ASA)
- Identity Services Engine (ISE)
- Cloud Web Security Services (CWS + WSA)
- Switches and Wireless Controllers
- Advanced Malware Protection
- NetFlow Collectors

NEW

Cisco AnyConnect

Integration with other Cisco solutions

NetFlow Collectors

© 2016 Cisco and/or its affiliates. All rights reserved.
Detect Suspicious Behavior More Effectively
AnyConnect Network Visibility Module (NVM) Enhancements

What’s New for ISE 2.1?
ISE 2.1 includes enhancements that deliver more flexibility in AnyConnect® NVM use. NVM enables greater visibility across users, endpoints, and applications, and facilitates analytics on contextual telemetry data.

Benefits
- Gain a holistic view across your entire network with greater insight from behavioral analytics and contextual data
- Defend more effectively against potential threats with greater visibility extended to all endpoints
- Improve network operations with forensic analysis to inform design, capacity planning, and troubleshooting

Gain Increased Visibility Across Your Network

Capabilities
- Stay informed with continuous monitoring and “always-on” capability that limits blind spots
- Collect and send data when on-premises and/or VPN-connected (including split tunneling)
- Get a 24-hour rolling cache of NetFlow data when disconnected
- Receive auditing intelligence with built-in reporting and analytics
- Limit impact on user experience with stream-level interception
- Benefit from flexibility and customization – e.g., collect only the attributes needed, cached data throttling
AC4.3 NVM New Features

- Flexible Collection Policy
- Throttling of Cached Data
- New Attributes
- Broadcast/Multicast Suppression
- Complete Attribute List
Currently AnyConnect ISE Posture Module verifies endpoint attributed at time of access or via reassessment window

**Continuous Monitoring** will be a new capability going forward from client
- USB check is the first
- More to come (e.g. continuous checking of applications)

**Opswat v4**
- Lots of new capabilities to leverage (e.g. Autoupdate)
Context Visibility
Gain a Deeper Understanding of Endpoint Activity
Context Visibility Enhancements

What’s New for ISE 2.1?
The ability to aggregate, store, and search high volumes of endpoint data, giving you greater visibility. ISE 2.1 collects data from multiple sources into one place, and its enhanced database stores more historical data than ever.

Benefits

Unified view
Access all of the endpoint data you need from one place

Simple, fast discovery
Get to the information you’re looking for in a few seconds

Deeper visibility
Perform detailed, retroactive forensic analysis after an endpoint has left the network

Capabilities

- Store data on 1.5 million endpoints across 50 attributes, not just endpoints that are currently active
- Benefit from in-disk storage (elastic search)
- Get insight more easily through a better user interface
- Perform forensic analysis on endpoints on the network in a previous week or month
- Import and export data as needed
- Aggregate endpoint information in one place

Logs
Syslogs
Reports
John on his iPad in Building 8 has Vulnerability <XYZ>
Context Visibility Wizard

Setup in a few clicks:

Get to know the devices and users' details of your network. Gain visibility and context with this setup wizard.

**Endpoints discovery**

We are going to discover the endpoints using the IP range(s) below.

- **IP address range**: Enter the IP range. E.g., 10.10.10.1/24 or 10.10.10.1 - 10.10.10.55

Add another range
Context Visibility – Stores current state of all endpoints

Import
Create/Update/Delete
REST API

Search
Visibility
Dashboard
Export
REST API

User, Endpoint, Network, Posture, Profile,
Location, Threat, Vulnerability, Custom Attributes

~50 default attributes out of the box
Expanded Profiling Capabilities

ISE now supports a new Active Directory probe and SMB discovery providing definitive operating system information eliminating guesswork. Custom ports, service and version information provide better information to shrink the pool of devices that stubbornly defy classification.
Dashboard Enhancements
Get the Information You Need Faster Than Ever
Dashboard Customization and Workflow Enhancements

What’s New for ISE 2.1?
Enhanced reporting and easier customization using dashlets to quickly adjust and create views that fit your specific needs. New task-oriented work centers for guest, BYOD, posture, profiling, and network access.

Benefits
- See the details that matter to you
- Easily create your own single pane of glass for quick insights
- Integrate with existing analytics
- Connect with your office analytics through Excel exports
- Get things done more easily
- Use new work centers to accelerate core activities

Capabilities
- Build custom dashboards; user controls what to view
  - Add, remove, and rename tabs and dashboard components ("dashlets")
  - Adjust layout – reorder dashlets, select from layout templates, and drag and drop dashlets
- Export to Excel and PDF
- Use new task-oriented work centers focused on BYOD, posture, and profiling

Director of Security
Security Engineer
NOC Engineer
Each individual can customize the main screen easily and quickly

Three new work centers streamline management activities
Sample Dashlets

**Profiles**
- Endpoint Profile

- **unknown**: 5%
- **other**: 5%
- **cisco-device**: 5%
- **apple-device**: 6%
- **ce_x_yosemite-wos**: 6%
- **microsoft-workstation**: 10%
- **intel-device**: 10%
- **apple-iphone**: 19%
- **apple-device**: 19%
- **windows7-workstation**: 17%

**COMPLIANCE**
- **pending**: 21%
- **compliant**: 79%

**ASSETS**
- **BYOD**: 27634
- **Corporate**: 34599
- **Guest Device**: 487

Last refreshed: Tue Feb 02 2016 19:23:49 GMT-0800 (PST)
Threat-Centric NAC
Threat Centric NAC

Correlating Threat and Vulnerability Information to reduce Time to Remediate with ISE Network Fabric Visibility and Control

- Discover Vulnerable Embedded IOT Devices
- Automated containment of vulnerable endpoints based on CVE Score
- Immediate action on prioritized vulnerability to maximize SOC resources
What is Threat Centric NAC: Vulnerability

Security Assessment service leverages industry standards for Vulnerability and Threats. Vulnerable EndPoints based on **CVSS Scores**

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>User</th>
<th>IP Address</th>
<th>Vulnerabilities</th>
<th>Source</th>
<th>Score</th>
<th>Logical NAD Location</th>
<th>Connectivity</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>98:4B:4A:09:5A:28</td>
<td>Big_Boss</td>
<td>1.1.2.1</td>
<td>Microsoft Internet Explorer</td>
<td>Qualys</td>
<td>10.0</td>
<td>SJ19/Floor 3</td>
<td>Connected</td>
<td>ASBUT-M-20</td>
</tr>
</tbody>
</table>
What is Threat Centric NAC: Threat
Threat EndPoints based on *Incidents and Indicators*
EasyConnect
Simplify access management while maintaining security

Easy Connect

What’s New for ISE 2.1?
Easy Connect is a quick, flexible user authentication method that applies when endpoints don’t support 802.1X. Easy Connect monitors user login via Active Directory and maps the user’s identity to give access.

Benefits

- Flexible deployment that doesn’t require a supplicant or PKI, allowing ISE to issue COA for added security
- Increased visibility into active network sessions authenticated against AD
- Immediate value with no need to touch each endpoint or require users to authenticate again

Easy Connect merges RADIUS identity with AD Login identity to deliver differentiated access

- Network access device (NAD) without 802.1X
- Active Directory (AD) Login
- Identity mapping
- SXP speaker
- Publish to pxGrid
- Publish to pxGrid
- MnT

Capabilities

- Active-session monitoring across both AD and network logins
- Session maintenance from wired MAB clients to NADs
- Directory notification publication via pxGrid
- Address legacy and unsupported NADs with Cisco TrustSec®
- Assignment of VLANs, DACLs, SGTs, and more for users authorized via Easy Connect

EasyConnect, a Secure Alternative to Whitelisting

<table>
<thead>
<tr>
<th>Basic with whitelisting</th>
<th>Better and flexible with ISE EasyConnect</th>
<th>Most secure with integrated 802.1X, supplicants and certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td>Security</td>
<td>Security</td>
<td>Security</td>
</tr>
<tr>
<td>Complexity</td>
<td>Complexity</td>
<td>Complexity</td>
</tr>
</tbody>
</table>

Better and more secure with ISE EasyConnect.
EasyConnect

Passive Login, FULL Control (No 802.1X)

Identity Services Engine

User Mappings Derived from AD Logins

AD Logins

Microsoft Active Directory Domain Controllers

Network Access Devices w/o 802.1X

Rest of Network

Non-intrusive

Uses What’s Already There (AD)

Full Visibility/Control w/o Touching Endpoints

Faster, Simpler Deployments for software-defined segmentation

SXP
Enable Consistent Security Policy Across the Enterprise
Cisco TrustSec and Cisco ACI Policy Plane Integration

What’s New for ISE 2.1?
Integration of Cisco TrustSec® and Cisco ACI™ policy groups enables customers to address breach, segmentation, and compliance challenges by sharing policy groups between networks and data centers.

Benefits
- Unified security policy based on user, device, application, and threat state in group-based policies
- Simplified security management: Complementary group-based policy approaches simplify security design, operations, and compliance
- Consistent segmentation across data center, branches, users, and devices

Capabilities
Consistent security policy groups can be shared between Cisco TrustSec and Cisco ACI domains:
- Campus security groups can be used in Cisco ACI policies: Cisco ACI learns Cisco TrustSec Security Group Tags (SGTs), and these SGTs are available for use by the Cisco® Application Policy Infrastructure Controller (APIC) policy
- Endpoint groups (EPGs) can be used in campus policies: ISE retrieves EPGs and creates SGTs in harmony
With the new TrustSec / ACI Integration
ACI EPGs are now learned by ISE and are translated as SGTs which can be used by ISE policy.
TrustSec Integration
Make Policy Changes in a Flexible Manner
Cisco TrustSec Change Management and Workflow Capabilities

**What’s New for ISE 2.1?**
New change management capabilities enable you to test changes to Cisco TrustSec® security policy before deployment, and to gradually deploy changes to different parts of the network.

**Benefits**
- **Reduced risk**
  Reduce the likelihood of changes causing problems
- **Greater control**
  See impact of policy adjustments in a controlled environment and fine-tune them before deployment
- **Increased flexibility**
  Roll out policies when you want, where you want

**Stage and Test Policy Changes to Verify Impact, and Roll Out on Your Terms**

**Stage policy changes**

<table>
<thead>
<tr>
<th>Source</th>
<th>Protected Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR</td>
<td>PERMIT</td>
</tr>
<tr>
<td>Finance</td>
<td>DENY</td>
</tr>
<tr>
<td>BYOD Corp</td>
<td>DENY</td>
</tr>
<tr>
<td>BYOD Vendor</td>
<td>DENY</td>
</tr>
</tbody>
</table>

**Test and fine-tune**

**Deploy changes in production to all devices or a selected subset**

<table>
<thead>
<tr>
<th>Source</th>
<th>Protected Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR</td>
<td>DENY</td>
</tr>
<tr>
<td>Finance</td>
<td>DENY</td>
</tr>
<tr>
<td>BYOD Corp</td>
<td>PERMIT</td>
</tr>
<tr>
<td>BYOD Vendor</td>
<td>DENY</td>
</tr>
</tbody>
</table>

**Capabilities**
- Modify SGACLs using a staging matrix and test them before pushing to production
- View changes in comparison to the production matrix
- Achieve seamless integration with ISE RBAC
- Choose to apply changes to all Cisco TrustSec enabled network devices or only to selected devices
- Request and gain approval for policy changes using a new workflow

C97-736227-01 © 2016 Cisco and/or its affiliates. All rights reserved.
TrustSec Workflow Enhancements

Offers a staging mechanism to allow the policy changes in the workflow mode with an option to not commit and download those changes on the TrustSec enabled network devices.
TrustSec Workflows

- TrustSec Workflows Enhancements

  Introduces capabilities for change management and configuration rollback as well as gradual deployment of new policies to different parts of the network that allow simplified integration of TrustSec into current IT systems.

  Seamless Integration with ISE RBAC which gives the ability for the ISE Administrator to create different roles like Editor and Approver for the Workflow process.

  Flexible option for the ISE administrator to enable and disable the workflow process for change management making it more relevant to the enterprise customers.
Device Administration
Unify Device Administration and Access Control
Enhanced Device Administration Support

What’s New for ISE 2.1?
ISE now includes all of the core device administration capabilities found in ACS, delivering contextual awareness and device administration capabilities in a single, central solution.

**Benefits**

- **Richer contextual policies**
  Build policies informed by contextual data from devices, infrastructure, and services

- **Flexible, granular control**
  Control and audit network device configuration

- **Unified, centralized management**
  Get a full view of all policy elements in a single management console

**Capabilities**

- Migration tool automatically migrates ACS configuration data to ISE
- Support for core ACS5 features and dedicated device administration work center supporting TACACS+
- Command-level authorization with detailed logs for auditing
- Dynamic role-based access control (RBAC)
- Discover, identify, and monitor all IP-enabled endpoints

Manage Device Administration and Access Control Policies in a Single Place

3rd Party, Compliance, BYOD, pxGrid & Guest
3<sup>rd</sup> Party NAD Phase 2

- Auth VLAN & DNS Sink-holing
  - Removes Requirement for URL Redirection
  - Supports all Flows:
    - Hotspot
    - CWA
    - BYOD
    - Posture Remediation
- SNMP CoA
New 2.1 Compliance Capabilities

- Microsoft Intune Integration
- Microsoft SCCM Integration (as MDM)
- Posture Workcenter
- USB Real Time Check
New 2.1 BYOD Capabilities

- BYOD Workcenter
- Pre-Canned BYOD Configurations - <10 Minutes to Stand Up BYOD:
  - CA & Certificate Templates
  - Client Provisioning Policies & NSPs PRE-LOADED
  - Identity Source Sequence & Authorization Rules
- Support for ChromeBook
- This is your cue for standing ovation
New 2.1 Guest Capabilities

- IdP-based Employee Login as Guest (BYOD, etc.)
- Support for any SAML 2.0 IdP
- Filtered Sponsor View (View Own Only)
- Finer Password Policy
- Web Proxy for SMS
- NIC Teaming for Portals
- From First Login - Yet another cue for standing ovation
The document describes the extensions made to Extensible Messaging and Presence Protocol (XMPP) [RFC5220] that enables the use of XMPP as a transport protocol for collecting and distributing any security telemetry information between and among network platforms, endpoints, and most any network connected device. Specifically, this document will focus on how these extensions can be used to transport the Incident Object Description Exchange Format (IODEF) information.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 8, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe the rights and restrictions with respect to this document. Code Components extracted from this document must include its

Cam-Winget, et al. Expires October 8, 2016 [Page 1]
ISE 2.1 GUI Demo