Simplify The Deployment & Management of Cisco TrustSec

Tejas Shah, Jay Bhansali
Some Webex Tips

- All participants will be placed on mute to avoid any unwanted noise during the presentations
- Use the Q and A window to ask questions
- If you are having technical difficulties, audio or visual, please use the Q and A window and we will try and fix them
- The presentation will be recorded for future playback and so you can share it with your peers
- A short survey will be sent at the end of the presentation, please provide your feedback
Objectives

At the end of this webinar, the participant should be able to:

- Understand Cisco’s TrustSec solution
- Understand the benefits of deploying the TrustSec solution to provide secure access control
- Understand how to use the Ciscoworks LAN Management System 4.0 to deploy the TrustSec solution
Agenda

- What is TrustSec?
- 802.1X Deployments
- TrustSec Differentiators
- TrustSec Best Practices
- Ciscoworks LMS 4.0
- Demo
The Need for TrustSec

- Complex workforce
- User and Device Mobility
- Device Proliferation
- Cloud/Virtualization

Questions:

1. Who are the users in my network?
2. What devices are in my network?
3. How do I enforce role-based access control?
4. How do I scale my access policy across my network?
Cisco TrustSec Architecture

Overlay/Appliance Mode  or  Infrastructure Integrated Mode

Identity Context
- User
- Contractor
- Guest
- Device Type
- Access Type
- Location
- Posture
- Time of Day

802.1X, Web Authentication, MAB Authentication Bypass, Profiling

Authorization and Enforcement
- Broad Access
- Limited Access
- Guest/Internet

VLAN, DACL, Security Group Access, Identity Firewall

Data Integrity and Confidentiality
MACSec (802.1AE)
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.

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

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

1. **End user / Endpoint attempts to access network**
   - 802.1X Authentication for registered user
   - MAC Authentication Bypass for agentless device
   - Web Authentication for Guest

2. **Policy Servers evaluate identity information**
   - Profiler evaluates agentless device
   - Guest Server manages temporary guest access
   - ACS evaluates overall policy and returns authorization back to NAD

3. **Authorize/Enforce based on policies**
   - Catalyst switches to enforce access control based on policy (VLAN Assignment, dACL, SGT)
   - Nexus 7000 to apply SGACL based on SGT mapped to role
**Cisco TrustSec Differentiators**
Flexible, Simplified Authentication

**Monitor Mode (Open Mode)**
Allows all traffic to pass through

IT administrator gets extended information for planning a 802.1X deployment

No impact on end-user

**Flex Auth**
Allows configuring the order and priority of 802.1X, MAB and Web-Authentication, on a per port basis.

Reduces Network Admin labor as one configuration fits all
Cisco TrustSec 1.0 Differentiators
Support for VM and Voice

Multi-Auth
Authenticated every mac address in the data domain

VMs on the host may use different mac addresses

Enforcement achieved using downloadable ACLs, with all traffic placed in default port VLAN

Multi-Domain Auth (MDA)
Allows for authentication & authorization of PC connected behind and IP phone

Phone traffic in tagged with the Voice Vlan ID

PC authenticates in Data domain and dACLs are applied based on applied policy

Phone authenticates in Voice Domain, tags traffic in Voice VLAN

PC authenticates in Data Domain, untagged traffic in data VLAN
TrustSec 802.1X Phased Approach

1. Monitor Mode
   - Primary Features:
     - Open mode
     - Multi-Auth
     - Flex Auth
   - Benefits:
     - Unobstructed Access
     - No Impact on Productivity
     - Gain Visibility AAA Logs

2. Low Impact mode
   - Primary Features:
     - Open mode
     - Multi-Domain
     - Port & dACLs
   - Benefits:
     - Maintain Basic Connectivity
     - Increased Access Security
     - Differentiated Access

3. High Security Mode
   - Primary Features:
     - Traditional Closed Mode
     - Dynamic VLANs
   - Benefits:
     - Strict Access Control
Best Practice for 802.1X Deployments

1. Include all IT departments in planning the TrustSec rollout – network security, infrastructure, desktop (supplicants) and support
2. Start off in monitor mode to gain better visibility into your network
3. Move to low-impact mode once you have determined how enabling 802.1X will impact your users
4. Supplicant selection - supplicant selection is important to pick the right EAP method that supports your security policy and the backend databases for the environment
5. Access Technologies (WOL/PXE) - understand the impact of VLAN assignment on desktop automation technologies and that there are choices in the design of the solution
6. Cisco ACS 5.2 release helps you to manage network access and will help to troubleshoot problems
7. Use CiscoWorks LMS 4.0 to assess infrastructure readiness and device configuration
TrustSec 1.0 Portfolio
802.1X Infrastructure Deployment

Policy Administration & Management
Access Control Solution
Cisco Works LMS

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

Client
NAC Agent
Web Agent
802.1X Supplicant
No-Cost Persistent & Temporal Clients for Posture, & Remediation
AnyConnect or OS-Embedded Supplicant
## Minimum Releases for TrustSec Identity Features

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexible authentication sequencing</td>
<td>12.2(50)SE</td>
<td>12.2(50)SG</td>
<td>12.2(33)SXI</td>
<td>ACS 5.2</td>
</tr>
<tr>
<td>IEEE 802.1X with open access</td>
<td>12.2(50)SE</td>
<td>12.2(50)SG</td>
<td>12.2(33)SXI</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.1X, MAB, and web authentication with downloadable ACL</td>
<td>12.2(50)SE</td>
<td>12.2(50)SG</td>
<td>12.2(33)SXI</td>
<td></td>
</tr>
<tr>
<td>Cisco Discovery Protocol enhancement for second-port disconnect</td>
<td>12.2(50)SE</td>
<td>12.2(50)SG</td>
<td>12.2(33)SXI</td>
<td></td>
</tr>
<tr>
<td>Inactivity timer for IEEE 802.1X and MAB</td>
<td>12.2(50)SE</td>
<td>12.2(50)SG</td>
<td>12.2(33)SXI</td>
<td></td>
</tr>
<tr>
<td>Multidomain authentication</td>
<td>12.2(25)SEC</td>
<td>12.2(31)SG</td>
<td>12.2(33)SXI</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.1X with multiauth</td>
<td>12.2(50)SE</td>
<td>12.2(50)SG</td>
<td>12.2(33)SXI</td>
<td></td>
</tr>
<tr>
<td>Centralized web authentication</td>
<td>12.2(50)SE</td>
<td>12.2(50)SG</td>
<td>12.2(33)SXI</td>
<td></td>
</tr>
<tr>
<td>Common session ID</td>
<td>12.2(50)SE</td>
<td>12.2(50)SG</td>
<td>12.2(33)SXI</td>
<td></td>
</tr>
</tbody>
</table>
TrustSec Benefits

Business Productivity and Collaboration
• Rapid service and application deployment
• Enable flexible collaboration
• IT consumerization support for productivity and next-gen workforce

Security Risk Management
• Network visibility and control
• Endpoint health for security
• Audit trails for compliance and monitoring

Opex Benefits
• Simplified network design and deployment
• Services embedded in the infrastructure
• Rapid audit resolution
TrustSec and CiscoWorks LMS 4.0

“Provides an extensible framework enabling large-scale lifecycle management of Cisco technologies and solutions”

- Simplify technology and solution adoption
- Centrally organizes Day 1-to-n management tasks
  - Contextual status & monitoring dashboards
  - Readiness assessment and remediation
  - Instructional configuration workflows

<table>
<thead>
<tr>
<th>Work Center</th>
<th>Configuration</th>
<th>Monitoring &amp; Reporting</th>
</tr>
</thead>
</table>
| EnergyWise     | Large-scale switch configuration  
 Manage EW domains and policies                                                  | Power consumption, Cost savings,  
 policy compliance, alarms & events                                                    |
| Identity       | Large-scale Identity deployment  
 Day-N configuration changes                                                       | ACS integration: Auth success failure  
 trends, user info, login stats                                                       |
| Smart Install  | Centrally manage Smart Install Directors  
 Manage client switch configuration and sw images                                 | Smart Install-specific LMS job  
 management                                                                               |
| Auto Smartports| Large-scale ASP deployment and day-N  
 configuration changes  
 Event/trigger management  
 MAC-based group configuration                                                       | Auto Smartports-specific LMS job  
 management                                                                               |
Demo
Thank you.