Posture Assessment with ISE

György Ács
Consulting Systems Engineer, C|EH – Cisco

T-SECA4
Prošíme, ptejte se nás

- Twitter  www.twitter.com/CiscoCZ
- Talk2cisco  www.talk2cisco.cz/dotazy
- SMS  721 994 600
ISE as a Posture Assessment

Analysis of Antivirus, Antispyware, personal FW processes … quarantine and remediation services + passive reassessment

ISE with NAC functionality
About Posture Assessment

**Authentication**
- Authenticate User
- Authenticate PC corporate asset?
- Authenticate Guests (WEB)
- Profile Devices, MAB

**Posture**
- Compliance Check OS, Hotfix, Antivirus, Personal Firewall
- Quarantine
- Remediation Fix problem, make PC compliant

**Authorization**
- Create different Zones to segment network
- Assign VLAN to port
- Assign ACL to port
# NAC appliance vs. ISE
802.1X authentication + posture + profiling + guest

<table>
<thead>
<tr>
<th>NAC Appliance</th>
<th>Description</th>
<th>ISE – NEW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks</td>
<td>File, Service, Registry, AV/AS checks</td>
<td>Posture Conditions</td>
</tr>
<tr>
<td>Rules</td>
<td>Multiple simple conditions are built together</td>
<td>Compound Posture Conditions</td>
</tr>
<tr>
<td>Requirements</td>
<td>Requirements are used with Operating Systems. They contain compound conditions. Each Requirement has a selected Remediation action.</td>
<td>Posture Requirements</td>
</tr>
<tr>
<td>Role Requirements</td>
<td>Posture policies can be evaluated based on Identity Groups, OS, and dictionary attributes. Policies contain the Requirements</td>
<td>Posture Policy</td>
</tr>
</tbody>
</table>
Posture Assessment in Wired and Wireless environments
802.1X End User Authentication with Posture

Supplicant / Posture Agent

Layer 2 Point-to-Point

802.1X Start

EAPOL-Start

EAPOL ID-Request

EAPOL ID-Response

EAP Transaction

EAP-Success

Posture Status: Unknown
Access: Limited

Authenticator

Layer 3 Link

Authentication Server

ise.demo.local

802.1X Authentication Authorization

RADIUS-Request

RADIUS-Request

RADIUS Authorization: EMPLOYEE-PRE-POSTURE
[cisco-av-pair] = dACL=PRE-POSTURE-ACL
[cisco-av-pair] = url-redirect-acl=REDIRECT-ACL

URL-Redirect

Flow continues to next slide

Redirect 302: https://ISE.DEMO.LOCAL:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp

https://ISE.DEMO.LOCAL:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp

Redirect 302: https://ISE.DEMO.LOCAL:8905/auth/discovery?sessionId=SessionIdValue

https://ISE.DEMO.LOCAL:8905/auth/discovery?sessionId=SessionIdValue

Posture/Downloader URL

Access-Accept

Flow continues to next slide
802.1X End User Authentication with Posture

Supplicant / Posture Agent

Posture Start

Layer 2 Point-to-Point

Posture Discovery

EAP-Success

Posture Negotiation, Agent Updates

Posture Request / Requirement

Posture Report (Result: Compliant)

Layer 3 Link

Access-Accept

ise.demo.local

Authentication Server

CoA + ReAuth

Change of Authorization Request

CoA ACK/NAK

802.1X Re-Authentication

Posture Status: Compliant
Access: Full-Access

Access-Accept

Reassessment

Posture Status

Posture Compliant

SWISS UDP/8905
Clients and provisioning
Global Client Provisioning and Posture Options

- General Settings
- Reassessments
- Updates
- Acceptable Use Policy
Policy Based Acceptable Use Policy

Acceptable User Policy

* Configuration Name: Guest
Configuration Description: AUP for
Show AUP to Agent users: (for Agent and Web Agent on Windows only)
  - Use URL for AUP message
  - Use file for AUP message (Please upload a zip file. The zip file must:
  * AUP URL: http://www.budlabsec.c

1. Posture AUP is not applicable for guest portal login (use guest AUP)
2. Each configuration must have a unique group or a unique configuration name.
3. No two configurations may have any group in common.
4. If a config already exists with a group of 'Any', then no other config may have that group.
5. If a config with a group of 'Any' must be created, delete all other configs with 'Any' group.

* Select User Identity Groups: Guest

Per User Identity Group

Existing Acceptable Use Policy Configurations
- Guest

User Identity Groups
- Guest
What else is needed?

- Agents
  - MAC OSX, Windows and WebAgent
- Compliance Module
- Agent Customization package
- Agent profile -> user interface

Resource files from local disk or Cisco site
Agent Profile

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Parameter Value</th>
<th>Mode</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN detect interval in secs (VlanDetectInterval): (0-900)</td>
<td>0</td>
<td>merge</td>
<td></td>
</tr>
<tr>
<td>Enable VLAN detect without UI? (EnableVlanDetectWithoutUI)</td>
<td>no</td>
<td>merge</td>
<td></td>
</tr>
<tr>
<td>Disable Agent exit? (DisableExit)</td>
<td>no</td>
<td>merge</td>
<td></td>
</tr>
<tr>
<td>Allow CRL checks? (AllowCRLChecks)</td>
<td>yes</td>
<td>overwrite</td>
<td></td>
</tr>
<tr>
<td>Accessibility mode? (AccessibilityMode)</td>
<td>no</td>
<td>merge</td>
<td></td>
</tr>
<tr>
<td>Check signature? (SignatureCheck)</td>
<td>no</td>
<td>merge</td>
<td></td>
</tr>
<tr>
<td>Bypass summary screen? (BypassSummaryScreen)</td>
<td>yes</td>
<td>merge</td>
<td></td>
</tr>
<tr>
<td>MAC exception list (ExceptionMACList)</td>
<td></td>
<td>merge</td>
<td></td>
</tr>
<tr>
<td>Discovery host (DiscoveryHost)</td>
<td></td>
<td>overwrite</td>
<td></td>
</tr>
<tr>
<td>Discovery host editable? (DiscoveryHostEditable)</td>
<td>yes</td>
<td>overwrite</td>
<td></td>
</tr>
<tr>
<td>Server name rules (ServerNameRules)</td>
<td></td>
<td>overwrite</td>
<td></td>
</tr>
<tr>
<td>Generated MAC (GeneratedMAC)</td>
<td></td>
<td>overwrite</td>
<td></td>
</tr>
<tr>
<td>Language info (Locale)</td>
<td>default</td>
<td>merge</td>
<td></td>
</tr>
<tr>
<td>Posture report filter (PostureReportFilter)</td>
<td>displayFailed</td>
<td>merge</td>
<td></td>
</tr>
</tbody>
</table>

Separated Profiles for Windows and OSX
NAC Agent (Persistent)

- Windows or MAC
- Localized (ISE 1.1 : 10 languages)
- Installed from Web or MSI
- Handles user logon
- Single-Sign-On: 802.1X
- Checks Posture
  - Remediates Posture
  - Guides user through process
  - Automatic remediation
  - Refreshes IP address
- Automatic update of the agent via ISE

Typical Use Case: Managed Devices
Agent Customization Package

Cisco NAC Agent

nac_login.xml

platformStrings_xx.xml

branding package
NAC Web Agent

- Windows
- Temporary (ActiveX)
- User logon
- Checks Posture
- Limited Remediation
- Refreshes IP address

Typical Use Case: Unmanaged PCs, Guests, Contractors
Provisioning based on Policy

Policy states: Enabled, Disabled, Monitor

First-match policy will be selected when there are multiple matches

Agent specification is mandatory, other resources are optional

Provision policy based on endpoint operating system user identity group dictionary based conditions
ISE – Provisioning Posture Agents

End user clicks to provision posture agent. Agent type and version based on ISE NAC Agent (persistent) and Web Agent (temporal).
Posture elements and features
Posture Assessment Elements

- File
- Registry
- Applications
- Service
- Compound Cond.
- AntiVirus
- AntiSpyware
- Custom Conditions

Cisco Predefined Checks for File, Registry, Application, Service, Compound, and AV, AS compound Conditions + User defined
Dictionary Simple Conditions

- Originally: empty
- Frequently used (dictionary) conditions make the policy easy
A dictionary compound condition is a logical combination of more than one dictionary simple condition (a dictionary attribute that is associated with a value).

It is a set of dictionary simple conditions (dictionary attributes that are associated with values) that are logically combined with an AND, or an OR operator.
A compound condition includes one or more simple conditions, or compound conditions of the type file, registry, application, service, or dictionary conditions.

You can combine one or more conditions using an **AND** (ampersand [ & ]), an **OR** (horizontal bar [ | ]), or a **NOT** (exclamation point [ ! ]) operator to create a compound condition.
Preconfigured Conditions, 300+
File, Registry, Application, Service, Compound, and AV, AS compound Conditions

Does PC have IE installed?

Registry Condition
- Name: pc_IE9_0
- Description: Cisco Predefined Check: Critical Up
- Registry Type: RegistryValue
- Registry Root Key: HKLM
- Value Name: Version
- Value Data Type: String
- Value Data: 9.0
- Operating System: Windows 7 (All) or Windows Vista (All)
Requirements

Predefined AV/AS requirements

Easy requirement fine-tuning
Default AV, AS, Installation and Definition Condition

AV (Any) is needed

Max 5 days old AV definition file
Create a Requirement

- **Name**
- **Operating Systems (OR)**
  - Example:
- **Conditions (AND)**
  - Operator
  - Condition types
    - Simple conditions
    - Compound conditions
- **Remediation**
  - Action
  - Message
Remediation types:
- **Automatic**—The NAC Agents automatically updates Windows clients with the latest WSUS updates.
- **Manual**—The user manually updates the Windows client with the latest WSUS updates from a Microsoft-managed WSUS server, or from the locally administered WSUS server for compliance.
Launch Program Remediation

- Allows administrators to launch a qualified (signed) remediation program through the Agent. Multiple programs are permitted, and they are launched in the same sequence as specified by the administrator.

Note:

A valid digital signature signed by certificate is required if user in client machine does not have admin privileges.
Windows Update Remediation

- Allows administrators to check and modify Windows Update settings, and launch Windows Updater on client machines where users have Administrator privileges.
- The Windows Update remediation provides an Update button on the (persistent) Agent for remediation. When the end user clicks the Update button, the Agent launches the Automatic Updates Agent and forces it to get the update software from an external WSUS server.

WSUS remediation should be optional, it is a long process
# ISE Posture Assessment/Remediation

<table>
<thead>
<tr>
<th>Posture Assessment Options</th>
<th>NAC Agent for Windows</th>
<th>Web Agent for Windows</th>
<th>NAC Agent for Mac OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OS/Service Packs/Hotfixes Process Check</td>
<td>OS/Service Packs/Hotfixes Process Check</td>
<td>AV Installation</td>
</tr>
<tr>
<td></td>
<td>Registry Check</td>
<td>Registry Check</td>
<td>AV Version/AV Definition Date</td>
</tr>
<tr>
<td></td>
<td>File Check</td>
<td>File Check</td>
<td>AS Installation</td>
</tr>
<tr>
<td></td>
<td>Application Check</td>
<td>Application Check</td>
<td>AS Version/AS Definition Date</td>
</tr>
<tr>
<td></td>
<td>AV Installation</td>
<td>AV Installation</td>
<td>Windows Update Running</td>
</tr>
<tr>
<td></td>
<td>AV Version/AV Definition Date</td>
<td>AV Version/AV Definition Date</td>
<td>Windows Update Configuration</td>
</tr>
<tr>
<td></td>
<td>AS Installation</td>
<td>AS Installation</td>
<td>WSUS Compliance Settings</td>
</tr>
<tr>
<td></td>
<td>AS Version/AS Definition Date</td>
<td>AS Version/AS Definition Date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Update Running</td>
<td>Windows Update Running</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Update Configuration</td>
<td>Windows Update Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WSUS Compliance Settings</td>
<td>WSUS Compliance Settings</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remediation Options</th>
<th>NAC Agent for Windows</th>
<th>Web Agent for Windows</th>
<th>NAC Agent for Mac OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Text (Local Check)</td>
<td>Message Text</td>
<td>Message Text</td>
<td>AV Installation</td>
</tr>
<tr>
<td>URL Link (Link Distribution)</td>
<td>URL Link</td>
<td>URL Link</td>
<td>AV Version/Def Date</td>
</tr>
<tr>
<td>File Distribution</td>
<td>File Distribution</td>
<td>File Distribution</td>
<td>AS Installation</td>
</tr>
<tr>
<td>Launch Program</td>
<td>Launch Program</td>
<td>Launch Program</td>
<td>AS Version/Def Date</td>
</tr>
<tr>
<td>AV Definition Update</td>
<td>AV Definition Update</td>
<td>AV Definition Update</td>
<td></td>
</tr>
<tr>
<td>AS Definition Update</td>
<td>AS Definition Update</td>
<td>AS Definition Update</td>
<td></td>
</tr>
<tr>
<td>Windows Update</td>
<td>Windows Update</td>
<td>Windows Update</td>
<td></td>
</tr>
<tr>
<td>WSUS</td>
<td>WSUS</td>
<td>WSUS</td>
<td></td>
</tr>
<tr>
<td>AV Live Update (AS Live Update)</td>
<td>AV Live Update (AS Live Update)</td>
<td>AV Live Update (AS Live Update)</td>
<td></td>
</tr>
</tbody>
</table>
Posture Policy

- Posture Policies tie the Requirements to Identity Groups and other Conditions together to make a Policy.
- Once a User is Authenticated, Posture Policy is checked for the Identity Group/User.
- If Posture passes, users will be assigned a new Authorization Policy.

![Posture Policy Image](image-url)
### Posture Policy Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Identity Groups</th>
<th>Operating Systems</th>
<th>Other Conditions</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MyAppPolicy</td>
<td>Any</td>
<td>Windows All</td>
<td>(Optional) Dictionary Attr...</td>
<td>TEST</td>
</tr>
<tr>
<td></td>
<td>Policy_Check_Fo</td>
<td>Any</td>
<td>Mac OSX</td>
<td>(Optional) Dictionary Attr...</td>
<td>Any_AS_D...</td>
</tr>
<tr>
<td></td>
<td>Policy_Check_Fo</td>
<td>Any</td>
<td>Windows All</td>
<td>(Optional) Dictionary Attr...</td>
<td>Any_AS_D...</td>
</tr>
<tr>
<td></td>
<td>Policy_Check_Fo</td>
<td>Any</td>
<td>Mac OSX</td>
<td>(Optional) Dictionary Attr...</td>
<td>Any_AS_D...</td>
</tr>
<tr>
<td></td>
<td>Policy_Check_Fo</td>
<td>Any</td>
<td>Windows All</td>
<td>(Optional) Dictionary Attr...</td>
<td>Any_AS_D...</td>
</tr>
</tbody>
</table>

**Mandatory**—This option enforces the client to meet the posture requirement, otherwise no / restricted access.

**Optional**—The client can bypass the requirement, but can have network access.

**Audit**—This option checks the client for the posture requirement without notifying the user. It does not affect user network access.
Authorization Policy

Best Practice: Authz Policy rules should distinguish two compliance states
Session:PostureStatus: Posture = Compliant
Session:PostureStatus: Posture != Compliant (inc. Unknown and NonCompliant)

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Identity Groups</th>
<th>Other Conditions</th>
<th>Other Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiled Cisco IP Phones</td>
<td>Cisco-IP-Phone</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Domain_Computer</td>
<td>Any</td>
<td>demo.local:ExternalGroups</td>
<td>EQUALS demo.local/Users/Domain Computers</td>
<td>-</td>
</tr>
<tr>
<td>Employee</td>
<td>Any</td>
<td>demo.local:ExternalGroups</td>
<td>EQUALS demo.local/Users/employees</td>
<td>Employee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>Session:PostureStatus: EQUALS Compliant</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>Session:PostureStatus: NOT EQUALS Compliant</td>
<td></td>
</tr>
<tr>
<td>Contractor</td>
<td>Contractor</td>
<td>Session:PostureStatus: EQUALS Compliant</td>
<td>Guest</td>
<td>Posture_Reemediation</td>
</tr>
<tr>
<td>Guest</td>
<td>Guest</td>
<td>Session:PostureStatus: EQUALS Compliant</td>
<td>Guest</td>
<td>-</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Best Practice: Add remediation ACLs for Posture Status != Compliant
Policy Based Re-Assessment

- Configurable per Role = User ID group

Contains the following fields:
- Configuration Name: Policy
- Configuration Description: Policy
- Use Reassessment Enforcement: checkbox
- Enforcement Type: continue
- Interval: 60 minutes
- Grace Time: 5 minutes

Group Selection Rules:
1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless:
   i. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
   ii. the existing config with a group of 'Any' is deleted.
4. If a config with a group of 'Any' must be created, delete all other configs first.

Additional note: continue, logoff or remediate
Let’s configure it!
Let’s check the running firewall service
Posture Status Monitoring

<table>
<thead>
<tr>
<th>Time</th>
<th>Status</th>
<th>Details</th>
<th>Username</th>
<th>Endpoint ID</th>
<th>IP Address</th>
<th>Network Device</th>
<th>Device Port</th>
<th>Authorization Profiles</th>
<th>Identity Group</th>
<th>Posture Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 21, 11 01:35:43.142 AM</td>
<td>✔️</td>
<td></td>
<td><a href="mailto:gacs@cisco.com">gacs@cisco.com</a></td>
<td>00:0C:29:A9:C7:6C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Guest</td>
</tr>
<tr>
<td>Dec 21, 11 01:35:42.832 AM</td>
<td>✔️</td>
<td></td>
<td>00:30:05:9E:5B:10</td>
<td>00:30:05:9E:5B:10</td>
<td>10.1.1.51</td>
<td>sw</td>
<td>FastEthernet1/0/16</td>
<td>web-auth</td>
<td></td>
<td>Pending</td>
</tr>
<tr>
<td>Dec 21, 11 01:35:25.434 AM</td>
<td>✔️</td>
<td></td>
<td>00:0C:29:A9:C7:6C</td>
<td>00:0C:29:A9:C7:6C</td>
<td>10.1.1.53</td>
<td>sw</td>
<td>FastEthernet1/0/16</td>
<td>web-auth</td>
<td></td>
<td>Pending</td>
</tr>
<tr>
<td>Dec 21, 11 01:29:03.236 AM</td>
<td>✔️</td>
<td></td>
<td><a href="mailto:gacs@cisco.com">gacs@cisco.com</a></td>
<td>00:0C:29:A9:C7:6C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Guest</td>
</tr>
<tr>
<td>Dec 21, 11 01:28:41.192 AM</td>
<td>✔️</td>
<td></td>
<td>00:0C:29:A9:C7:6C</td>
<td>00:0C:29:A9:C7:6C</td>
<td>10.1.1.53</td>
<td>sw</td>
<td>FastEthernet1/0/16</td>
<td>web-auth</td>
<td></td>
<td>Pending</td>
</tr>
<tr>
<td>Dec 21, 11 01:28:31.622 AM</td>
<td>✔️</td>
<td></td>
<td>00:30:05:9E:5B:10</td>
<td>00:30:05:9E:5B:10</td>
<td>10.1.1.51</td>
<td>sw</td>
<td>FastEthernet1/0/16</td>
<td>web-auth</td>
<td></td>
<td>Pending</td>
</tr>
<tr>
<td>Dec 21, 11 01:20:18.194 AM</td>
<td>✔️</td>
<td></td>
<td><a href="mailto:gacs@cisco.com">gacs@cisco.com</a></td>
<td>00:0C:29:A9:C7:6C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Guest</td>
</tr>
<tr>
<td>Dec 21, 11 01:19:17.498 AM</td>
<td>✔️</td>
<td></td>
<td><a href="mailto:gacs@cisco.com">gacs@cisco.com</a></td>
<td>00:0C:29:A9:C7:6C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Guest</td>
</tr>
<tr>
<td>Dec 21, 11 01:18:08.938 AM</td>
<td>✔️</td>
<td></td>
<td>00:0C:29:A9:C7:6C</td>
<td>00:0C:29:A9:C7:6C</td>
<td>10.1.1.51</td>
<td>sw</td>
<td>FastEthernet1/0/16</td>
<td>web-auth</td>
<td></td>
<td>Pending</td>
</tr>
<tr>
<td>Dec 21, 11 01:17:51.800 AM</td>
<td>✔️</td>
<td></td>
<td>00:0C:29:A9:C7:6C</td>
<td>00:0C:29:A9:C7:6C</td>
<td>10.1.1.53</td>
<td>sw</td>
<td>FastEthernet1/0/16</td>
<td>web-auth</td>
<td></td>
<td>Pending</td>
</tr>
</tbody>
</table>
Posture Log

User2, Windows 7 64 bits, Av McAfee, Antispyware, MS and McAfee, result: compliant
Posture Reports

- Posture Report (Monitor -> Reports -> Catalog -> Posture)
Best Practices, considerations

- **Design Posture:** Describe posture policy requirements for endpoint compliance. This may include many areas such as asset checking, application and services checking, and antivirus and antispyware checks, as well as customized checks for specific use cases. Describe remediation plans and include remediation servers that need to be integrated into the design.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>OS (Windows /MacOS)</th>
<th>Conditions</th>
<th>Posture Agent</th>
<th>Checks</th>
<th>Remediation</th>
<th>Enforcement (Audit/Opt/ Mandatory)</th>
<th>When Assessed (Login/PRA/Both)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee_AV</td>
<td>Windows XP/7</td>
<td>AD group= Employee</td>
<td>NAC Agent for Windows</td>
<td>AV Rule: Microsoft Security Essentials 2.x</td>
<td>Live update (Automatic)</td>
<td>Mandatory</td>
<td>Both</td>
</tr>
<tr>
<td>Employee_Asset</td>
<td>Windows XP/7</td>
<td>AD group= Employee</td>
<td>NAC Agent for Windows</td>
<td>Custom registry check</td>
<td>Link redirect to policy page (Manual)</td>
<td>Mandatory</td>
<td>Login</td>
</tr>
<tr>
<td>Contractor_AV</td>
<td>Windows ALL</td>
<td>ID Group= Contractor</td>
<td>Web Agent</td>
<td>AV_Rule: Any AV w/current signatures</td>
<td>Local Message regarding AV Policy</td>
<td>Mandatory</td>
<td>Login</td>
</tr>
</tbody>
</table>
Summary

• Integrated Posture Assessment
  Part of TrustSec
  Standard 802.1X and Posture
  Policy based provisioning
  Wired, wireless and VPN*
  Corporate users (802.1X) and Guest (WebAuth)
  Leveraged NAC Appliance architecture

• Flexible configuration
  Preconfigured policy set
  User configurable policies

\[ \int_{a}^{b} f(x) \, dx \]
Otázky a odpovědi

- Twitter  www.twitter.com/CiscoCZ
- Talk2Cisco  www.talk2cisco.cz/dotazy
- SMS  721 994 600

- Zveme Vás na **Ptali jste se…** v sále LEO
  1.den 17:45 – 18:30
  2.den 16:30 – 17:00
Prosíme, ohodnoťte tuto přednášku.