White Paper

Cisco Catalyst Access Switching: Cat2K, Cat3K, Cat4K Series with ISE Solution – General Guidelines And Best Practices White Paper

Sanjay Shah - sshah@cisco.com
Wafo Tengueu - ltengueu@cisco.com

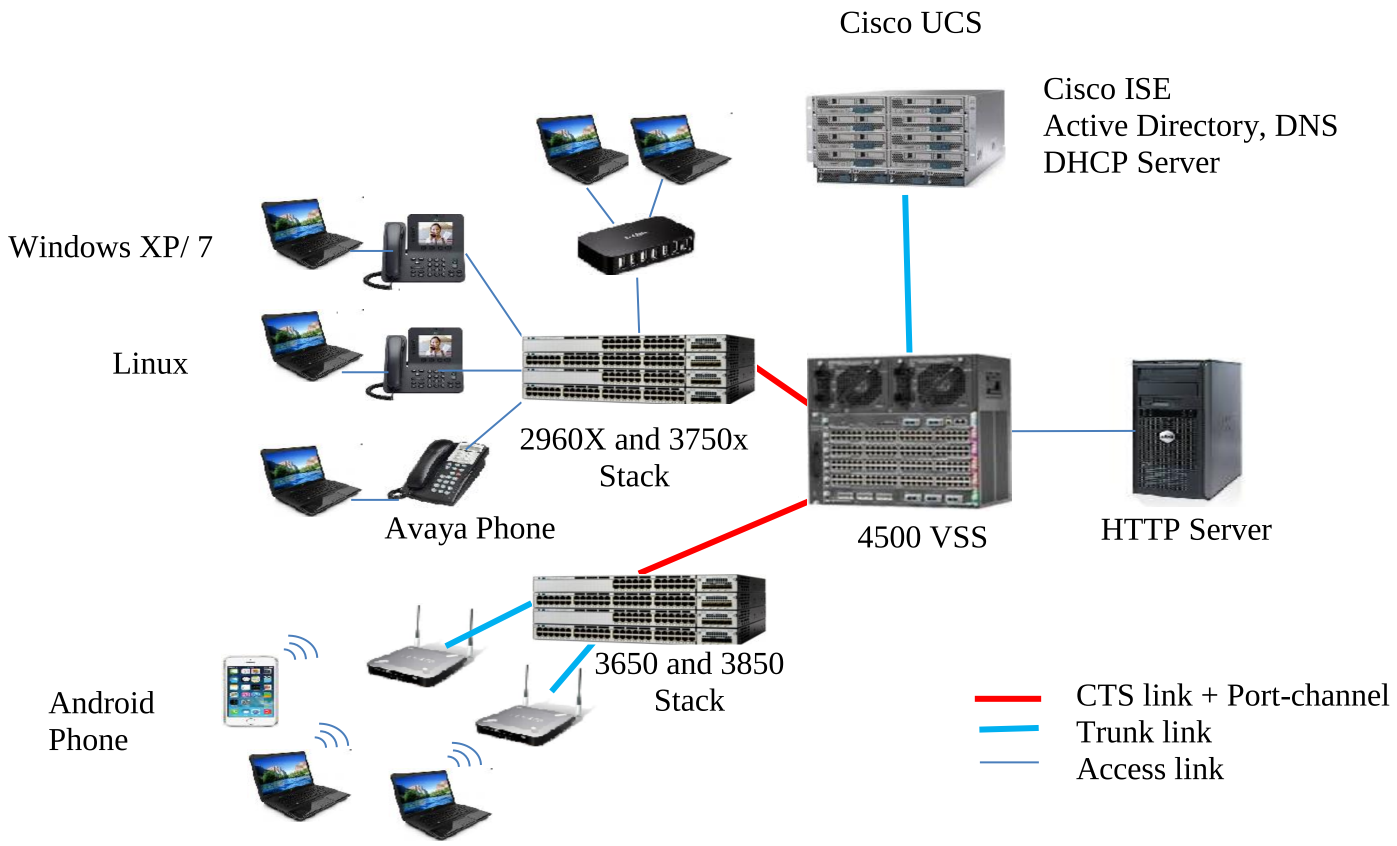
Table of Contents

Cisco Catalyst Access Switching: 1
Cat2K, Cat3K, Cat4K Series with 1
ISE Solution – General Guidelines 1
And Best Practices White Paper 1
Table of Contents 2
Introduction 3
ISE Solution Topology 3
Simulated Test Topology 4
HW Details 5
Test Approach and Methodology 5
Authentication and Authorization Use Cases 6
PACL, VACL, DACL Use Cases 6
Policies Use Cases 7
HA/SSO and Feature Interaction Use Cases 7
Scale, Performance and Longevity Use Cases 8
Timer Considerations 10
2960X, 3650-3850, and 4K-Sup8 Maximum Scale Numbers 11
Sample AAA Config 12
Sample Interface Config – Legacy Mode 13
Sample Interface Template Config – eEdge Mode 14
Glossary of Acronyms 17
Conclusion 18
References 19

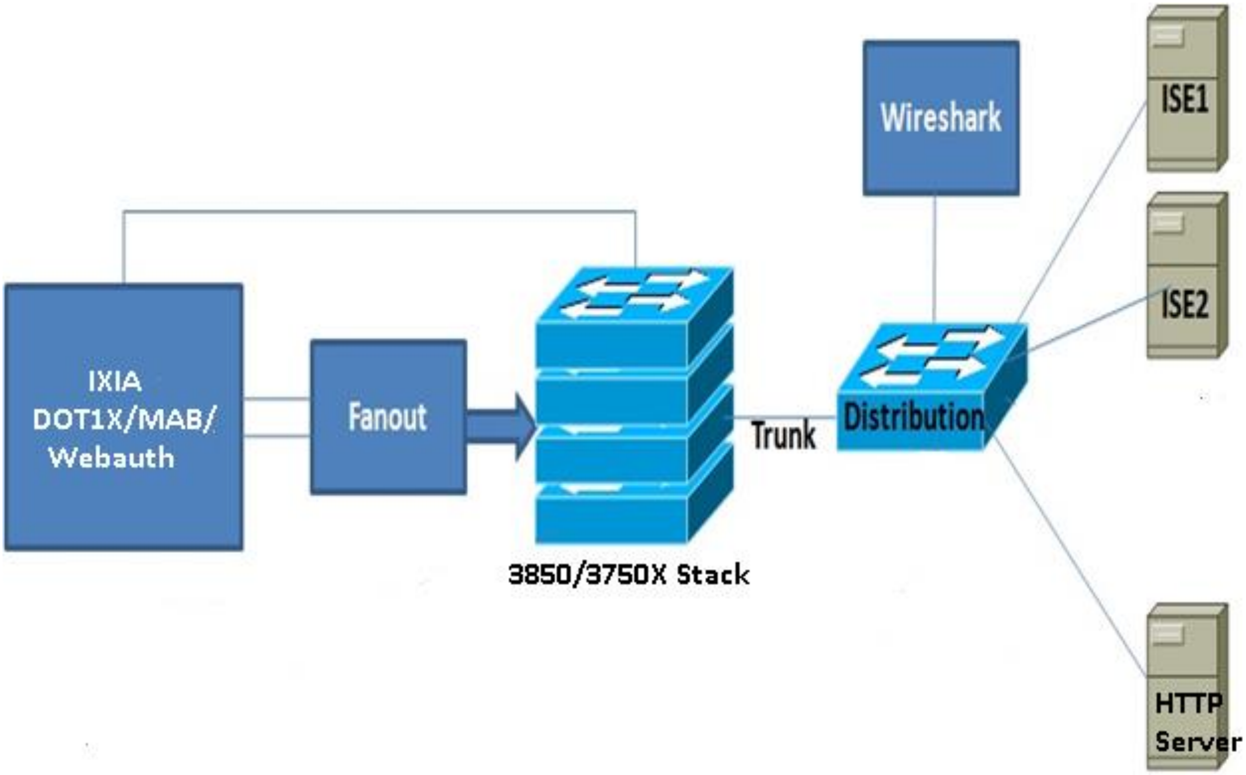
Introduction

The Cisco® Identity Services Engine (ISE) is the market-leading platform for security-policy management. It unifies and automates highly secure access control to proactively enforce role-based access to enterprise networks and network resources. The purpose of this document is to present general guidelines on ISE solution with 2K, 3K, 4K series access switching platform. This document is intended to help customers understand the critical elements of ISE solution that was validated in Cisco lab for release 15.2(2)E3 (3.6.3) together with ISE 1.3 patch 3. The recommendations in this document will help our customers with successful deployments. At the end of the document there are additional references to configuration and design guides, ISE compatibility matrix, and Cisco TrustSec.

ISE Solution Topology



Simulated Test Topology



HW Details

Hardware / Devices	Software
4500 VSS: WS-X45-SUP7-E, WS-X4748-RJ45V+E, WS-X4748-UPOE+E	15.2(2)E3 - 3.6.3
3850 Stack (5-member): WS-C3850-48T, WS-C3850-24P	15.2(2)E3 - 3.6.3
3750X Stack (6-member): WS-C3750X-48P, WS-C3750X-48, WS-C3750X-24P	15.2(2)E3 - 3.6.3
2960X Stack (3-member)	15.2(2)E3 – 3.6.3
Access Points: AIR-CAP2602E-A-K9	
ISE: UCS240	1.1 and 1.3
HTTP/HTTPS Server: UCS240	Linux
Client Simulator: IXIA Optixia x16	IxOS 6.60
Client Simulator - Pagent: 3825, 3845	Pagent 5.0.0
PC Clients: Lenova laptops 4xx	Windows 7
VM Clients	Windows XP, Linux
Voice Clients: Cisco 7961, 7962, 7975, 7942, CP-9971 and Avaya	
Android Clients: C2305	Android 4.2.2
iPhone Clients: Apple iPhone	iOS
Windows Clients: Samsung	Windows 7.5
Axis Camera and Cisco IP Camera CIVS-IPC-4500, Cisco Telepresence Tandberg Telecom AS	
Web Clients	Firefox, IE, Chrome

Test Approach and Methodology

- Simulate base traffic of ~1500 Dot1X/MAB/Webauth sessions
- Use real wired and wireless phones, PCs, PCs behind phone, tablets in tests
- Validate Authentication and Authorization with various wired and wireless clients
- Verify Memory and CPU utilization at various test points
- Verify PACL, VACL, DACL and Policy use cases
- Verify Feature interaction use cases
- Perform scale, performance and longevity use cases

Authentication and Authorization Use Cases

- Local authentication with configured username, password, radius attributes and ACL
- Local authentication with different authentication profiles - PEAP/LEAP/TLS/EAP-FAST/MD5
- Remote authentication with various host modes (single-host, multi-host, multi-domain, multi-auth)
- PCs, Laptops, Phones, PC behind phones - data and voice domains configured in same VLAN and different VLANs
- Webauth with gateway for that VLAN terminating on a different switch
- Authentication with multiple ISE servers and load balancing
- Supplicant Switch authenticates with Authenticator Switch using dot1X over single-host trunk port with Client Information Signalling Protocol (CISP) enabled
- Authentication - client moved from one supplicant switch to another
- Authentication and authorization on multiple uplink ports on different ASIC
- Change of Authorization (CoA) on Multi-Authentication (MA) and Multi-Domain Authentication (MDA) ports, single-host and multi-host
- Local Web Authentication (LWA) and Centralized Web Authentication (CWA)
- Custom Webauth, Consent and Webconsent (login, failure, success) with and without virtual IP in Apple and Android devices
- External Webauth, Consent and Webconsent with fin-wait timer in iPad, Andriod and Windows devices
- Captive Bypass Portal with HTTPS in iPad and Android devices with Webauth, Consent and Webconsent
- Webauth, Consent and Webconsent with and without Virtual IP (VIP)
- Extensible Authentication Protocol (EAP) chaining with username and password
- EAP chaining with security certificates (TLS)
- IPV6 Webauth, Consent, and Webconsent
- Port security with voice and data clients
- Mac move: Data host moving from one port to another
- Host presence: Data host disconnect behind IP phone
- SSH / TACACS

PACL, VACL, DACL Use Cases

- DACL programmed in hardware for every wired authenticated and authorized client: Dot1X PC, MAB PC, Dot1X Phones, MAB Phones
- DACL programmed in hardware for every wired and wireless authenticated and authorized client: Two AP with wireless clients connected to ASIC 0 and ASIC 1
- Simultaneously download of DACL policies with remark on multiple MA and MDA ports
- Per-User ACL for 20 Dot1X users on single MA port

- PACL/VACL/DACL policy co-existing on ingress - traffic is filtered based on the order ACLs are applied (PACL, VACL and then DACL)
- DACL downloaded only for Data client on MDA mode (no DACL for voice)
- Client access - fully qualified domain name (FQDN) ACL with multiple domain names
- Download different DACL/Filter-ID for multiple sessions on the MA ports
- Download 64 ACE DACL for multiple sessions on the MA port
- Per user ACL for data users

Policies Use Cases

- VLAN policy changes for existing sessions during re-authentication
- Filter-ID on multiple MA and MDA ports
- Security Tag (SGT) on multiple MA and MDA ports and single-host (Note: In Multi-host only first host is visible, all other hosts get tagged with same SGT)
- Local policy precedence change over server policy and vice versa
- Policy replace, replace all and merge as part of re-authentication
- Concurrent Dot1X, MAB, and Web Authentication policy
- SXP speaker and listeners
- SGACL enforcement on 3750X, 3850 and 4500
- Multiple CTS Dot1X links (L2, L3 and ether-channel) between Cat3K and Cat4k with various Security Association Protocol (SAP) modes (gcm-encrypt, gmac, null and no-encap)

HA/SSO and Feature Interaction Use Cases

- HA with radius port connected to Master unit - authentication after reload
- Webauth fails due to wrong credentials or timeout and fallback to MAB authentication
- Client stays authorized and accessible (critical auth) to network if AAA server is dead
- Open authentication in single host mode with authentication violation replace
- CDP Bypass - Phones and PC connected to port with authentication - host mode as single-host and multi-host
- DHCP IP’s released and renewed - IP is released from one client and another client re-uses the same IP address
- Input queue counters appropriately increment/decrement with central Webauth profile configured on ISE for MAB clients
- Client mac address re-learnt on the new port with re-authentication. If mac-move is disabled the new port will not learn the mac address and will result in security violation
- Guest VLAN clients initiate EAP but doesn’t respond to EAP-Request
- Traffic permitted/denied based on VLAN map for restricted VLAN (auth-fail vlan)
- Critical VLAN for new and existing session on MA and MDA ports with local re-auth timer configured – validate user profile in effect

- Critical Voice VLAN for new and existing session on MA and MDA ports with local re-auth timer configured
- Existing pre-Critical Auth authorized clients still authorized with local/user profile and continue to send traffic with un-reachable AAA
- Re-trigger authentication for Critical Auth session when AAA becomes alive
- Client get new IP during DHCP renew on MA and MDA ports - traffic is allowed from clients as per DCAL policy
- Idle timeout change on ISE for existing sessions for various timeout values
- Inactivity timeout for existing sessions for various timeout values
- Authorize multiple users on same MA port with various DACL and Filter-Id name lengths
- Clear auth session on switch stack when authentication/authorization in progress
- Multiple Linksec sessions on MA ports
- Host mode changes from Single-Host (SH) > Multi-domain > Multi-Host (MH) > Multi-authentication
- Re-apply same interface template multiple times on same MA and MDA ports
- Re-apply same service template multiple times on same MA and MDA ports
- Logout Window Disabled, Success Window Disabled on iPad, Android and Windows devices with Webauth, Consent and Webconsent
- Webauth with Virtual IP and Virtual Host – Virtual Host is seen in URL redirect
- Intercept-https-disabled – HTTPS should not redirect
- Un-configure policy map for authenticated session – Devices should not allow
- Custom Webauth, Consent, and Webconsent with image name length greater than custom page name length for login, success and failure pages
- Centralized Web Authentication (CWA) with Dot1X
- Webauth DACL with Change of Authorization (CoA)
- 2000 HTTP/HTTPS invalid/empty credentials
- Empty username and password in Apple and Android devices
- Change Virtual IP (VIP) for authenticated session and logout
- Convert Legacy Authentication (authentication convert new-style)
- Webauth after MAP authorization
- Accounting start, stop and update records
- Perform IOS upgrade (ISSU) from various releases to 3.6.3 (15.2(2)E3)

Scale, Performance and Longevity Use Cases

- 1000 Dot1X sessions, 1000 MAB sessions - sessions, memory (Auth Mgr, Dot1X, EPM, FED, FFM) and CPU validated
- Download large DACL (64 ACEs) for multiple Dot1X users on Single MA port
- 2048 open TCP connections with Webauth clients
- Centralized Web Authentication (CWA) with 2048 bytes redirect URL length with second mac-filtering - URL should be automatically redirected

- Local Web Authentication (LWA) with 550 bytes redirect URL - URL redirected
- 25 domain names in Fully Qualified Domain Name (FQDN) list
- 2000 Authenticated sessions with 2000 HTTP/HTTPS requests
- Re-authenticate 2000 sessions with re-auth timer
- Simulate continuous Dot1X Authentication failure (~500 sessions with **correct credentials**) for 8 hours on Access Reject with 10 sec re-authentication timeout.
- Simulate continuous Dot1X Authentication failure (~500 sessions with **in-correct credentials**) for 8 hours on Access Reject with 10 sec re-authentication timeout.
- Simulate continuous Dot1X Authentication failure (~500 sessions) for 8 hours due to no response from Radius server.
- Simulate continuous switching between Critical Auth and Radius Auth by making AAA sever reachable and un-reachable for 8 hours
- Simulate continuous Authentication failure due to missing and/or wrong Cisco AV-pair in Radius response for 8 hours
- Simulate continuous Authorization failure due to fail to apply VLAN policy (VLAN is disabled on switch) for 8 hours
- Simulate continuous Authorization failure due to fail to apply DACL/Filter-Id policy (ISE sends in-correct ACE in DACL) for 8 hours
- Simulate continuous Authorization policy replace and replace all (AAA attribute) for valid authorization for 8 hours
- Simulate continuous wired Authorization policy merge (AAA attribute) for valid authorization for 8 hours
- Simulate Extensible Authentication Protocol over LAN (EAPOL) at 1000 PPS for 8 hrs
- Simulate HTTP/HTTPS request from PCs for 2000 users with missing credentials (username and/or password) for 8 hours
- Send HTTP/HTTPS request from Andriod and Apple device with missing credentials (username and/or password) for 8 hours
- Simulate continuous wireless HTTP/HTTPS Webauth Authentication incomplete due to no response from external webserver for 8 hours
- Clear session (IP admission cache) and shut WLAN with 2000 wireless Webauth HTTP/HTTPS sessions
- Clear sessions after converting Legacy Webauth to eEdge mode on all ports
- Bring-up 2000 sessions and perform re-auth for all sessions
- Continuously flap link with 500 Dot1X and MAB sessions for 8 hours
- Simulate incomplete Dot1X authentication (no response from Client for Radius-Challenge) for 8 hours
- Simulate 100 Dot1X and MAB sessions with member ports and perform 20 switchover
- Simulate 100 wireless Webauth sessions with member ports and perform 20 switchover
- Simulate bulk MAB (phone) and Dot1X (PC) login and logout
- Bring up 2000 Dot1X sessions at 100 CPS on 192 ports

Timer Considerations

Switch CLI	Default	Comments
radius-server timeout	5 sec	**Use default settings**. If you configure both global and per Radius server timeout, the per-server timer will override global timer. Please note, switch will attempt to reach radius server three times after which it will timeout – (3 X 5 sec = 15 sec).
authentication periodic	Disabled	Enable on port if you like to set reauthentication timer on the switch or to have the switch use a RADIUS-provided session timeout. **Radius provided timeout is more scalable and easier to manage.**
authentication timer inactivity	Disabled	**After enabling periodic re-authentication on a port**, if there is no activity from the client for the set time then client is unauthorized
authentication timer reauthenticate	3600 sec	**After enabling periodic re-authentication on a port**, an automatic re-authentication attempt is initiated after timer expiry. **When periodic re-authentication is not enabled on a port** it sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request.
authentication timer restart	60 sec	**After enabling periodic re-authentication on a port**, an attempt is made to authenticate an unauthorized port after timer expiry

2960X, 3650-3850, and 4K-Sup8 Maximum Scale Numbers

Scale Test	2960X	3650 / 3850	4K-Sup8
Maximum VLANs	1000		4094
Maximum class-maps per policy-maps	63	255 User Defined +1 Default	254
Maximum class-maps per system	128	13260	2047
Maximum egress policers	NA	63	16384
Maximum ingress policers	510	63	16384
Maximum Dot1x OR MAB clients sessions	2000	2000	4000
Maximum Web Authentication sessions		2000	4000
Maximum Dot1X sessions with Critical Auth VLAN enabled and server reinitialize	2000	2000	5112
Maximum Dot1X sessions with service templates OR session features applied	2000	2000	4000
Maximum MAB sessions with various session features applied	2000	2000	4088
Maximum supported Dot1X OR MAB sessions	2000	2000	4000
Maximum output QoS entries	NA	1544	304
Maximum input & output table map markings for CoS and ToS	NA	14	512 for COS 2 for TOS

P.S.: For clients/end devices test tool simulation was used over few ports.

Sample AAA Config

```
>>>
!
!
aaa authentication login default none
aaa authentication dot1x default group ISE
aaa authorization exec default none
aaa authorization network default group ISE
aaa accounting auth-proxy default start-stop group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting delay-start all
aaa accounting update periodic 120
!
!
aaa server radius dynamic-author
 client 172.25.51.8 server-key cisco
!
!
radius server ISE
 address ipv4 172.25.51.8 auth-port 1812 acct-port 1813
 timeout 2
 retransmit 3
 pac key cisco
!
!
aaa group server radius ISE
 server name ISE
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server retransmit 5
radius-server accounting system host-config
radius-server deadtime 10
radius-server dead-criteria time 5 tries 3
!
>>>
```

Configure CTS Credentials from enable promt for CTS Dot1x links / NDAC:

```
Switch#  cts credentials id <device ID> password <password>
```

Sample Interface Config – Legacy Mode

```
>>>
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 16
 ip device tracking maximum 2
 trust device cisco-phone
 authentication event fail action next-method
 authentication event server dead action authorize vlan 100
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order dot1x mab webauth
 authentication priority dot1x mab webauth
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication violation protect
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 10
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
!
!
>>>
```

Sample Interface Template Config – eEdge Mode

```
>>>
!
!
service-template webauth-global-inactive
 inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template FAIL_OPEN_ACL
 description Service template for Fail open mode
 access-group ISE-ACL-ALLOW
 tag FAIL_OPEN_ACL
service-template ISE-ACL-DEFAULT
 access-group ISE-ACL-DEFAULT
service-template ISE-ACL-ALLOW
 access-group ISE-ACL-ALLOW
!
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match result-type aaa-timeout
 match authorization-status authorized
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match result-type aaa-timeout
 match authorization-status unauthorized
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 match activated-service-template FAIL_OPEN_ACL
!
class-map type control subscriber match-all MAB
 match method mab
```

```
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 match activated-service-template FAIL_OPEN_ACL
!
!
policy-map type control subscriber IDENTITY-POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   15 activate service-template FAIL_OPEN_ACL
   20 authorize
   30 pause reauthentication
  10 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  20 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   30 authenticate using mab priority 10
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 10
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   30 authorize
   40 authentication-restart 60
  50 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
```

```
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
 event violation match-all
  10 class always do-until-failure
   10 restrict
!
!
>>>
```

Glossary of Acronyms

CISP	Client Information Signalling Protocol
CoA	Change of Authorization
CoS	Class Of Service
CTS	Cisco TrustSec
CWA	Centralized Web Authentication
DACL	Downloadable Access Control List
DHCP	Dynamic Host Configuration Protocol
Dot1X	802.1x
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
EAPOL	Extensible Authentication Protocol over LAN
FQDN	Fully Qualified Domain Name
ISE	Identity Search Engine
LEAP	Lightweight Extensible Authentication Protocol
LWA	Local Web Authentication
MA	Multi-Authentication
MAB	MAC Authentication Bypass
MD5	Message Digest Algorithm 5
MDA	Multi-Domain Authentication
MH	Multi-Host
PACL	Port Access Control List
PEAP	Protected Extensible Authentication Protocol
QoS	Quality Of Service
SAP	Security Association Protocol
SGACL	Security Group Access Control List
SGT	Security Tag
SH	Single-Host
SSH	Secure Shell
SXP	SGT Exchange Protocol
TACACS	Terminal Access Controller Access-Control System
TLS	Transport Layer Security
ToS	Type of Service
VACL	VLAN Access Control List
VIP	Virtual IP
Webauth	Web Authentication
Webconsent	Web Consent

Conclusion

The use cases exercised in Cisco lab provides a base understanding on ISE solution capabilities. This effort reflects Cisco IOS release **3.6.3 (15.2(2)E3)** with **ISE 1.3 patch 3**.

Some key observations and recommendations:

- Dot1X support requires an authentication server such as ISE. Dot1X authentication does not work unless the network access switch can route packets to the configured ISE server. In closed mode, until a client is authenticated, only Extensible Authentication Protocol over LAN (EAPOL) traffic (and/or CDP if enabled) is allowed through the port to which the client is connected. After authentication succeeds, normal traffic can pass through the port.
- **It is recommended to use downloadable ACL (DACL) instead of static ACLs** on the switch. In a small branch converged access design it is easier to apply uniform access policy from a centralized ISE policy server rather than configuring on every access switch in the network. Changes to the access list control entries only have to be configured within the Cisco ISE server versus having to touch all campus switches.
- **It is recommended to restrict dynamic ACLs (DACL) to less than 64 ACEs per DACL** so that it gives maximum compatibility across different switching platforms, configurations, network topologies and ISE servers. While it might be possible to achieve stable configuration with greater than 64 ACEs in some cases, the recommendation of 64 ACEs is made such that the ACL is compatible in a majority of scenarios.
- **It is recommended to use Centralized Web Authentication (CWA)** with the ISE whenever possible. There are a few scenarios where LWA is preferred or the only option. For CWA or LWA process to work, a client needs to be able to obtain the: IP address; Default route; DNS server. All of these can be provided with DHCP or the local configuration. **The DNS resolution needs to work in order for the CWA or LWA to work.**
- For client https traffic to be intercepted and redirection to work, HTTP(S) needs to be enabled on the Cat3850 switch.
- Permit/Deny statements in the Redirect ACL carry different meaning i.e. For redirect ACL, – ‘permit’ means what packets are punted to CPU for processing i.e. essentially allowing for redirection, ‘deny’ means what packets are forwarded through hardware but not subjected to redirection, ‘rest’ of the packets are dropped.
- DNS server resolution is mandatory for url-redirection to work for Apple iOS devices.
- In certain endpoints such as iOS devices, there is no need for Supplicant Provisioning Wizard (SPW) package because the native operating system is used to configure the Dot1X settings.
- It is important to note, for Android devices the user is required to download the software (SPW) from Google's Play Store, since it cannot be distributed by ISE.

References

Catalyst 3650 Series Switch Platform Configuration Guide, Cisco IOS XE 3.6E

Catalyst 3850 Series Switch Platform Configuration Guide, Cisco IOS XE 3.6E

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, Cisco IOS XE 3.6.0E and IOS 15.2(2)E

ISE Design Guides

ISE 1.3 Compatibility Chart

Cisco TrustSec

Identity-Based Networking Services 2.0 Deployment Guide