Introduction

This document describes how to configure the Cisco Identity Services Engine (ISE) to provide full access to the network only when USB mass storage devices are disconnected.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Adaptive Security Appliance (ASA) CLI configuration and Secure Socket Layer (SSL) VPN configuration
- Basic knowledge of remote access VPN configuration on the ASA
- Basic knowledge of ISE and posture services

Components Used

Cisco Identity Services Engine (ISE) version 2.1 along with AnyConnect Secure Mobility Client 4.3 supports USB Mass Storage Check and Remediation. The information in this document is based on these software versions:

- Cisco ASA software Versions 9.2(4) and later
Microsoft Windows Version 7 with Cisco AnyConnect Secure Mobility Client Version 4.3 and later
- Cisco ISE, Release 2.1 and later

Configure

Network Diagram

Windows 7, Anyconnect 4.3

ASA Firewall

ISE 2.1

The flow is the following:

- User is not connected to VPN yet, private USB Mass Storage device is plugged in and content is available for the user
- VPN session initiated by AnyConnect client is authenticated via ISE. Posture status of the endpoint is not known, rule "PostureUnknown" is hit and as a result the session will be redirected to the ISE
- The USB checks introduces a new class of checks in AC ISE posture, in that they will continuously monitor the endpoint as long as it remains in the same ISE controlled network. The only logical remediation action available is to block the USB device(s) identified by their drive letter
- VPN session on ASA is updated, redirect ACL is removed and full access is granted

VPN session has been presented just as an example. Posture functionality is working fine also for other types of the access.

ASA

ASA is configured for remote SSL VPN access using ISE as AAA server. Radius CoA along with redirect ACL needs to be configured:

```
aaa-server ISE21 protocol radius
  authorize-only
  interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE21 (outside) host 10.48.23.88
```
key cisco

tunnel-group RA type remote-access
tunnel-group RA general-attributes
    address-pool POOL
    authentication-server-group ISE21
    accounting-server-group ISE21
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
group-alias RA enable

webvpn
    enable outside
    anyconnect image disk0:/anyconnect-win-4.3.00520-k9.pkg 1
    anyconnect enable
tunnel-group-list enable
    error-recovery disable
group-policy GP-SSL internal
group-policy GP-SSL attributes
dns-server value 10.62.145.72
    vpn-tunnel-protocol ssl-client

access-list ACL_WEBAUTH_REDIRECT extended deny udp any any eq domain
access-list ACL_WEBAUTH_REDIRECT extended deny ip any host 10.48.23.88
access-list ACL_WEBAUTH_REDIRECT extended deny icmp any
access-list ACL_WEBAUTH_REDIRECT extended permit tcp any any

For more details please refer to:

AnyConnect 4.0 Integration with ISE Version 1.3 Configuration Example

ISE

Step 1. Configure Network Device

From Administration > Network Resources > Network Devices > add ASA.
Step 2. Configure Posture conditions and policies

Make sure posture conditions are updated: Administration > System > Settings > Posture > Updates > Update now option.

ISE 2.1 comes with a preconfigured USB Condition, which checks if a USB mass storage device is connected.

From Policy > Policy Elements > Conditions > Posture > USB Condition verify existing condition:

From Policy > Policy Elements > Results > Posture > Requirements, verify preconfigured requirement which uses that condition.
From **Policy > Posture**, add a condition for all Windows to use that requirement:

From **Policy > Policy Elements > Results > Posture > Remediation Actions > USB Remediations** verify preconfigured remediation action to block USB storage devices:

Step 3. Configure Client Provisioning resources and policy

From **Policy > Policy Elements > Client Provisioning > Resources** download compliance module from Cisco.com and upload manually the AnyConnect 4.3 package:
Using **Add > NAC Agent or AnyConnect Posture Profile** create an AnyConnect Posture profile (name: *Anyconnect_Posture_Profile*) with default settings.

Using **Add > AnyConnect Configuration** add an AnyConnect Configuration (name: *AnyConnect Configuration*):

From **Policy > Client Provisioning** create a new policy (Windows_Posture) for Windows to use the AnyConnect Configuration:

**Step 4. Configure Authorization rules**

From **Policy > Policy Elements > Results > Authorization** add an Authorization Profile (name:
Posture_Redirect) that redirects to a default Client Provisioning Portal:

Note: ACL_WEBAUTH_REDIRECT ACL is defined on ASA.

From Policy > Authorization create an authorization rule for redirection. An authorization rule for Compliant devices is preconfigured on ISE:

If the endpoint is compliant, full access is provided. If status is unknown or noncompliant, redirection for Client Provisioning is returned.

Verify

Before VPN session establishment
USB device plugged in, and its content is available for the user.

**VPN session establishment**

During authentication, ISE will return redirect access-list and redirect url as part of Posture_Redirect Authorization Profile.
Once the VPN session is established, ASA traffic from the client will get redirected according to redirect access-list:

BSNS-ASA5515-11# sh vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : cisco Index : 29
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES128 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 14696 Bytes Rx : 18408
Pkts Tx : 20 Pkts Rx : 132
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GP-SSL Tunnel Group : RA
Duration : 0h:07m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a3042ca0001d00056e2dce3
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 29.1
Public IP : 10.229.16.34
Encryption : none Hashing : none
TCP Src Port : 61956 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 22 Minutes
Client OS : win
Client OS Ver: 6.1.7601 Service Pack 1
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 6701 Bytes Rx : 774
Pkts Tx : 5 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 29.2
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 61957
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 22 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 6701 Bytes Rx : 1245
Pkts Tx : 5 Pkts Rx : 5
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 29.3
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 55708
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes                Idle TO Left : 26 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 1294                                Bytes Rx : 16389
Pkts Tx : 10                                     Pkts Rx : 126
Pkts Tx Drop : 0                                 Pkts Rx Drop : 0

ISE Posture:
  Redirect URL : https://ISE21-1ek.example.com:8443/portal/gateway?sessionId=0a3042ca0001d00056e2dce3&portal=2b1ba210-e...  
  Redirect ACL : ACL_WEBAUTH_REDIRECT

Client Provisioning

At that stage, endpoint web browser traffic is redirected to ISE for client provisioning:

If needed, AnyConnect along with the Posture and Compliance module is updated.

Posture check and CoA

Posture module is executed, discover ISE (it might be required to have DNS A record for enroll.cisco.com to succeed), download and check posture conditions, new OPSWAT v4 block USB device action. Configured message will be displayed for the user:

Once the message is confirmed, USB device is no longer available for the user:
ASA removes redirection ACL providing full access. AnyConnect reports compliance:

![Cisco AnyConnect Secure Mobility Client](image)

Also detailed reports on ISE can confirm that required conditions are passed.

Posture Assessment by Condition:

![Posture Assessment by Condition](image)

Posture Assessment by Endpoint:
Details of Endpoint Report:

Troubleshoot

ISE is able to provide the details on the failing conditions, actions should be taken accordingly.

References

- Configuring an External Server for Security Appliance User Authorization
- Cisco ASA Series VPN CLI Configuration Guide, 9.1
- Cisco Identity Services Engine Administrator Guide, Release 2.0
- Technical Support & Documentation - Cisco Systems