

Configurar o 2.1 ISE e a verificação da postura USB de AnyConnect 4.3

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[ASA](#)

[ISE](#)

[Etapa 1. Configurar o dispositivo de rede](#)

[Etapa 2. Configurar condições e políticas da postura](#)

[Etapa 3. Configurar recursos e política do abastecimento do cliente](#)

[Etapa 4. Configurar regras da autorização](#)

[Verificar](#)

[Antes do estabelecimento da sessão de VPN](#)

[Estabelecimento da sessão de VPN](#)

[Abastecimento do cliente](#)

[Verificação da postura e CoA](#)

[Troubleshooting](#)

[Referências](#)

Introdução

Este original descreve como configurar o Cisco Identity Services Engine (ISE) para fornecer o acesso direto à rede somente quando os dispositivos de memória de massa USB são desligados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração de CLI da ferramenta de segurança (ASA) e da configuração de VPN adaptáveis do Secure Socket Layer (SSL)
- Conhecimento básico da configuração do acesso remoto VPN no ASA
- Conhecimento básico do ISE e dos serviços da postura

[Componentes Utilizados](#)

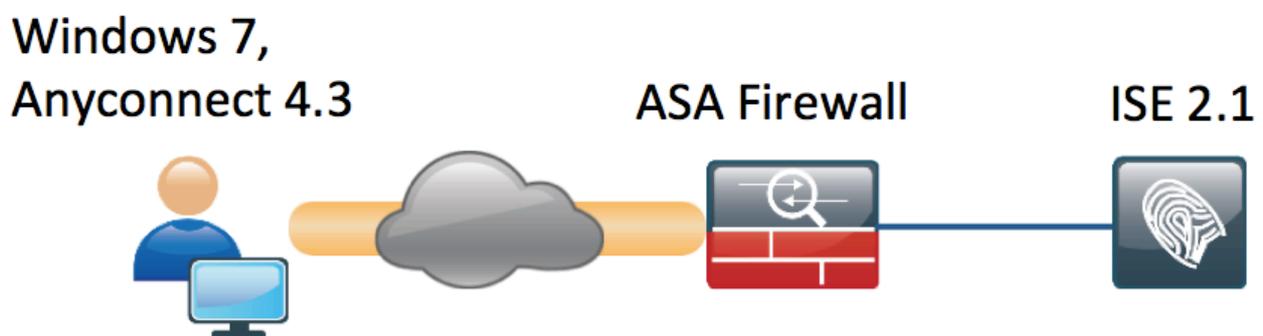
Versão 2.1 do Cisco Identity Services Engine (ISE) junto com a verificação e a remediação

seguras da memória de massa dos apoios USB do cliente 4.3 da mobilidade de AnyConnect. As informações neste documento são baseadas nestas versões de software:

- Versões de software de Cisco ASA 9.2(4) e mais atrasado
- Versão 7 de Microsoft Windows com versão 4.3 e mais recente do Cliente de mobilidade Cisco AnyConnect Secure
- Cisco ISE, 2.1 da liberação e mais tarde

Configurar

Diagrama de Rede



O fluxo é o seguinte:

- O usuário não é conectado ao VPN ainda, o dispositivo de memória de massa privado USB é obstruído dentro e satisfeito está disponível para o usuário
- A sessão de VPN iniciada pelo cliente de AnyConnect é autenticada através do ISE. O estado da postura do valor-limite não é sabido, a regra "Posture_Unknown" é batida e em consequência a sessão será reorientada ao ISE
- As verificações USB introduzem uma classe nova de verificam dentro a postura C.A. ISE, que monitorem continuamente o valor-limite enquanto permanece na mesma rede controlada ISE. A única ação lógica da remediação disponível é obstruir os dispositivos USB identificados por sua letra da unidade
- A sessão de VPN no ASA é atualizada, reorienta o ACL é removida e o acesso direto é concedido

A sessão de VPN foi apresentada apenas como um exemplo. A funcionalidade da postura está trabalhando muito bem igualmente para outros tipos do acesso.

ASA

O ASA é configurado para o acesso remoto SSL VPN usando o ISE como o servidor AAA. O CoA do raio junto com reorienta o ACL precisa de ser configurado:

```
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 any
access-list ACL_WEBAUTH_REDIRECT extended permit tcp any any
```

Satisfaça para mais detalhes referem:

[Integração de AnyConnect 4.0 com exemplo de configuração da versão 1.3 ISE](#)

ISE

Etapa 1. Configurar o dispositivo de rede

Do > Add ASA da administração > dos recursos de rede > dos dispositivos de rede.

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Network Devices List > BSNS-ASA5515-11

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

CoA Port

Etapa 2. Configurar condições e políticas da postura

Certifique-se que condições da postura está atualizada: **A administração > o sistema > os ajustes > a postura > atualizam > opção da atualização agora.**

O 2.1 ISE vem com uma condição preconfigured USB, que verifique se um dispositivo de memória de massa USB é conectado.

Da política > dos elementos da política > condiciona > postura > condição USB verificam condição existente:

The screenshot shows the Cisco Identity Services Engine interface. The navigation menu includes Home, Context Directory, Operations, Policy, Administration, and Work Centers. Under Policy, there are sub-menus for Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The Policy Elements menu is expanded to show Dictionaries, Conditions, and Results. The Conditions menu is further expanded to show various condition types, including Posture conditions like Anti-Malware, Anti-Spyware, Anti-Virus, Application, Compound, Disk Encryption, File, Patch Management, Registry, Service, and USB Condition. The main content area displays the details for the USB_Check condition:

- Name: USB_Check
- Description: Cisco Predefined Check: Checks if USB mass storage device is connected.
- Operating System: Windows All
- Compliance Module: 4.x or later

Da política > dos elementos da política > resultam > a postura > as exigências, verificam a exigência preconfigured que usa essa circunstância.

The screenshot shows the Cisco Identity Services Engine interface with the Requirements table visible. The navigation menu is the same as in the previous screenshot. The Requirements table is as follows:

Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
USB_Block	for Windows All	using 4.x or later	met if USB_Check	then USB_Block

Da política > da postura, adicionar uma condição para que todo o Windows use essa exigência:

Identity Services Engine Home > Context Directory > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name	Identity Groups	Operating Systems	Compliance Module	Other Conditions	Requirements
✓	Windows 7 USB check	If Any	and Windows 7 (All)	and 4.x or later	and	then USB_Block

Da política > dos elementos da política > resultam > as ações da postura > da remediação > as remediações USB verificam a ação preconfigured da remediação para obstruir dispositivos de armazenamento USB:

Identity Services Engine Home > Context Directory > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys > Conditions > Results

USB Remediations

Edit + Add Duplicate Delete

Name	Description	Type
<input type="checkbox"/> USB_Block	Cisco Predefined Remediation: ...	Automatic

- Authentication
- Authorization
- Profiling
- Posture
 - Remediation Actions
 - Anti-Malware Remediations
 - Anti-Spyware Remediations
 - Anti-Virus Remediations
 - File Remediations
 - Launch Program Remediations
 - Link Remediations
 - Patch Management Remediations
 - USB Remediations
 - Windows Server Update Services Remediations
 - Windows Update Remediations
 - Requirements
- Client Provisioning

Etapa 3. Configurar recursos e política do abastecimento do cliente

Da política > dos elementos da política > do abastecimento > dos recursos do cliente transfira o módulo da conformidade de Cisco.com e transfira arquivos pela rede manualmente o pacote de AnyConnect 4.3:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation menu includes Home, Context Directory, Operations, Policy, Administration, and Work Centers. Under 'Policy Elements', there are sub-menus for Authentication, Authorization, Profiling, Posture, and Client Provisioning. The 'Results' sub-menu is active, displaying a table of resources.

Name	Type	Version	Last Update	Description
<input checked="" type="checkbox"/> AnyConnectDesktopWindows 4.3.520.0	AnyConnectDesktopWindows	4.3.520.0	2016/03/11 11:10:47	AnyConnect Secure Mobility Clie...
<input checked="" type="checkbox"/> AnyConnectComplianceModuleWind...	AnyConnectComplianceMo...	4.2.330.0	2016/03/11 11:11:16	AnyConnect Windows Complian...
<input type="checkbox"/> WinSPWizard 2.1.0.50	WinSPWizard	2.1.0.50	2016/03/07 17:50:37	Supplicant Provisioning Wizard f...
<input type="checkbox"/> AnyConnect Configuration	AnyConnectConfig	Not Applicable	2016/03/11 11:12:42	
<input type="checkbox"/> MacOsXSPWizard 2.1.0.39	MacOsXSPWizard	2.1.0.39	2016/03/07 17:50:37	Supplicant Provisioning Wizard f...
<input type="checkbox"/> Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/03/07 17:50:37	Pre-configured Native Supplicant...
<input type="checkbox"/> Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/03/07 17:50:37	Pre-configured Native Supplicant...
<input type="checkbox"/> Anyconnect_Posture_Profile	AnyConnectProfile	Not Applicable	2016/03/11 14:39:03	

Usar-se adiciona > agente NAC ou o perfil da postura de AnyConnect cria um perfil da postura de AnyConnect (nome: *Anyconnect_Posture_Profile*) com configurações padrão.

Usar-se adiciona > configuração de AnyConnect adiciona uma configuração de AnyConnect (nome: Configuração de AnyConnect):

The screenshot shows the configuration page for 'AnyConnect Configuration' in the Cisco Identity Services Engine (ISE) interface. The navigation menu is the same as in the previous screenshot. The 'Results' sub-menu is active, displaying the configuration details for the 'AnyConnect Configuration' resource.

AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package: AnyConnectDesktopWindows 4.3.520.0

* Configuration Name: AnyConnect Configuration

Description: [Text Area]

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 4.2.330.0

Notes

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Start Before Logon
- Diagnostic and Reporting Tool

Profile Selection

- * ISE Posture: Anyconnect_Posture_Profile
- VPN: [Dropdown]
- Network Access Manager: [Dropdown]
- Web Security: [Dropdown]
- AMP Enabler: [Dropdown]
- Network Visibility: [Dropdown]
- Customer Feedback: [Dropdown]

Da política > do abastecimento do cliente crie uma política nova (Windows_Posture) para que Windows use a configuração de AnyConnect:

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then WinSPWizard 2.1.0.50 And Cisco-ISE-NSP
Windows_Posture	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration
MAC OS	If Any	and Mac OSX	and Condition(s)	then MacOsXSPWizard 2.1.0.39 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

Etapa 4. Configurar regras da autorização

Da política > dos elementos da política > resulta > a autorização adiciona um perfil da autorização (nome: Posture_Redirect) que reorienta a um portal do abastecimento do cliente do padrão:

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authorization Profiles > Posture_Redirect

Authorization Profile

* Name: Posture_Redirect

Description: [Empty]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: ACL_WEBAUTH_REDIRECT Value: Client Provisioning Portal (defa)

Nota: ACL WEBAUTH REDIRECT ACL é definido no ASA.

Da política > da autorização crie uma regra da autorização para a reorientação. Uma regra da autorização para dispositivos complacentes preconfigured no ISE:

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

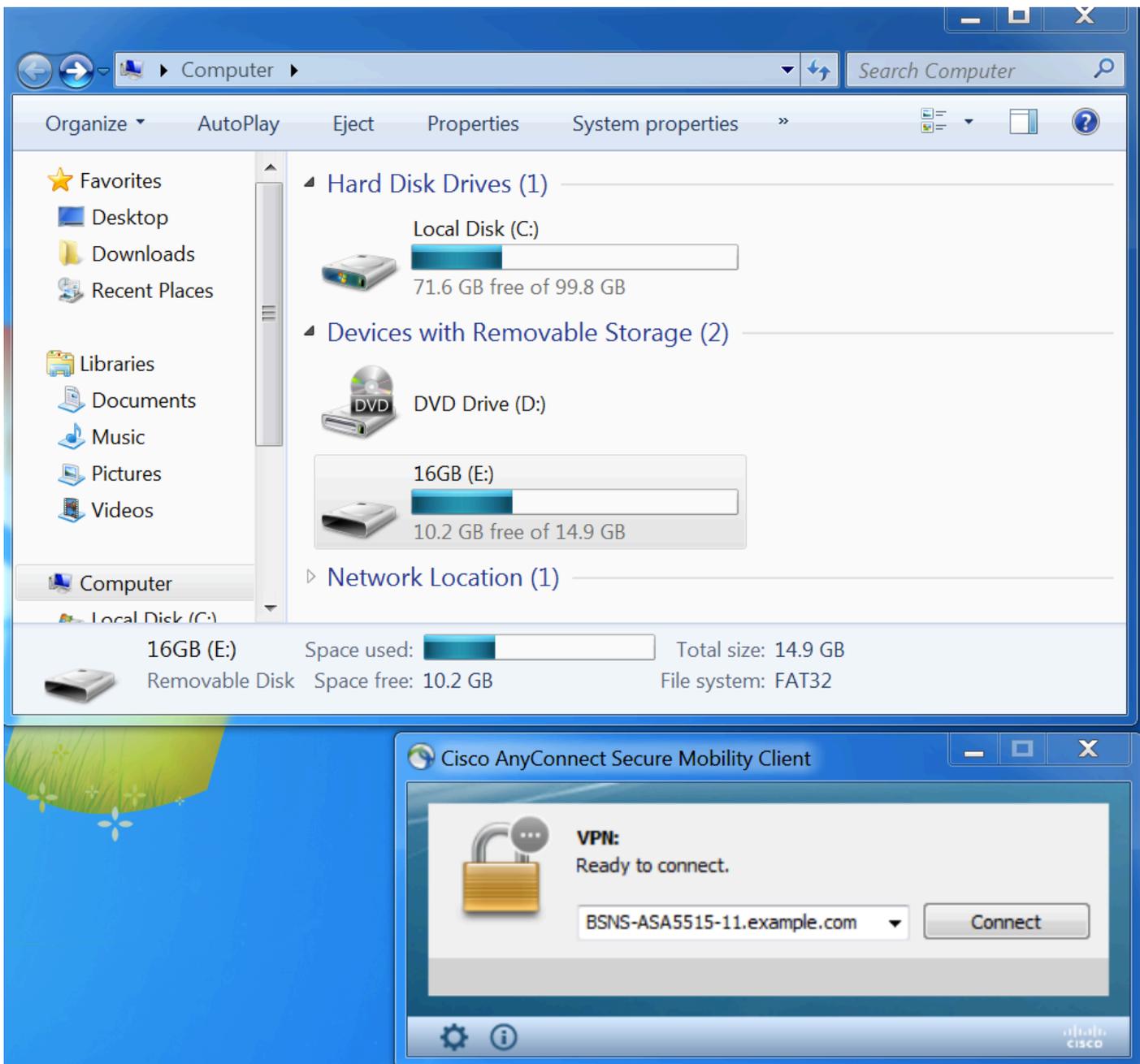
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
✔	Posture_Unknown	if Session:PostureStatus NOT_EQUALS Compliant	then Posture_Redirect

Se o valor-limite é complacente, o acesso direto está fornecido. Se o estado é desconhecido ou noncompliant, a reorientação para o abastecimento do cliente está retornada.

Verificar

Antes do estabelecimento da sessão de VPN

O dispositivo USB obstruído dentro, e seu índice estão disponíveis para o usuário.



Estabelecimento da sessão de VPN

Durante a autenticação, o ISE retornará reorienta a lista de acesso e reorienta a URL como parte do perfil da autorização de Posture_Redirect

Cisco Identity Services Engine											
RADIUS											
Misconfigured Supplicants		Misconfigured Network Devices		RADIUS Drops		Client Stopped Responding		Repeat Counter			
0		0		6		0		0			
Refresh Every 1 minute Show Latest 20 records Within Last 5 minutes											
Time	Sta...	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Pr...	IP Address	Network De...	Posture Status	Server
Mar 11, 2016 03:57:40.126 PM			cisco	00:0C:29:C9:...	Default >> Default >> Default	Default >> Posture_Un...	Posture_Redirect	10.10.10...		Pending	ISE21-1
Mar 11, 2016 03:57:39.598 PM			cisco	00:0C:29:C9:...	Default >> Default >> Default	Default >> Posture_Un...	Posture_Redirect		BSNS-ASA55...	Pending	ISE21-1

Uma vez que a sessão de VPN é estabelecida, o tráfego ASA do cliente obterá reorientado de

acordo com reorienta a lista de acesso:

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
Login Time : 15:57:39 CET Fri Mar 11 2016
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

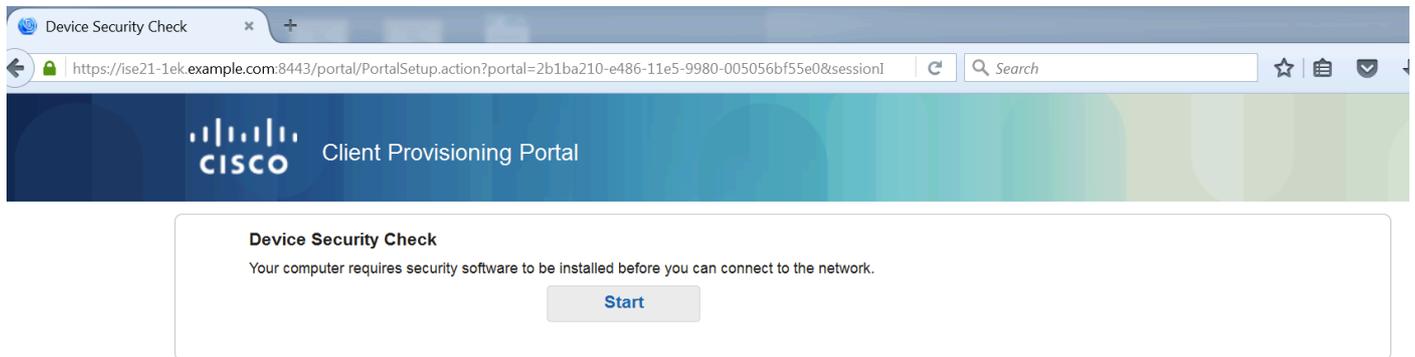
Idle Time Out: 30 Minutes Idle TO Left : 26 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 1294 Bytes Rx : 16389
Pkts Tx : 10 Pkts Rx : 126
Pkts Tx Drop : 0 Pkts Rx Drop : 0

ISE Posture:

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

Abastecimento do cliente

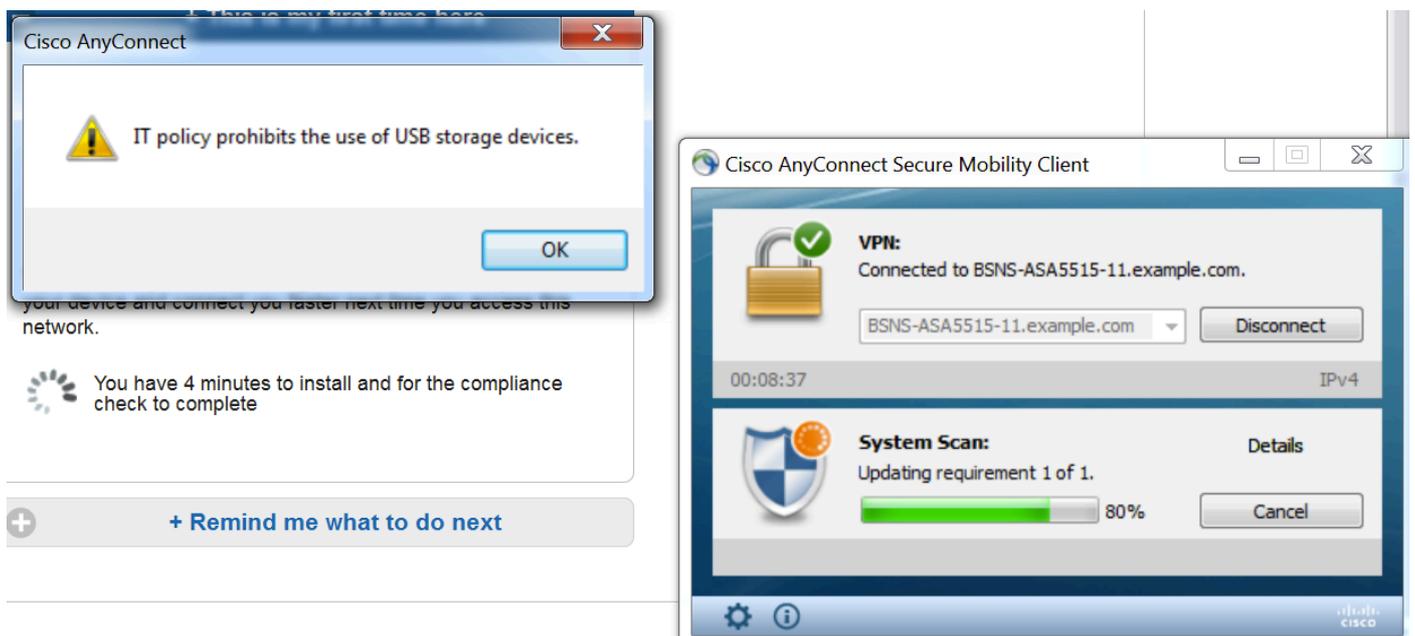
Nessa fase, o tráfego do web browser do valor-limite é reorientado ao ISE para o abastecimento do cliente:



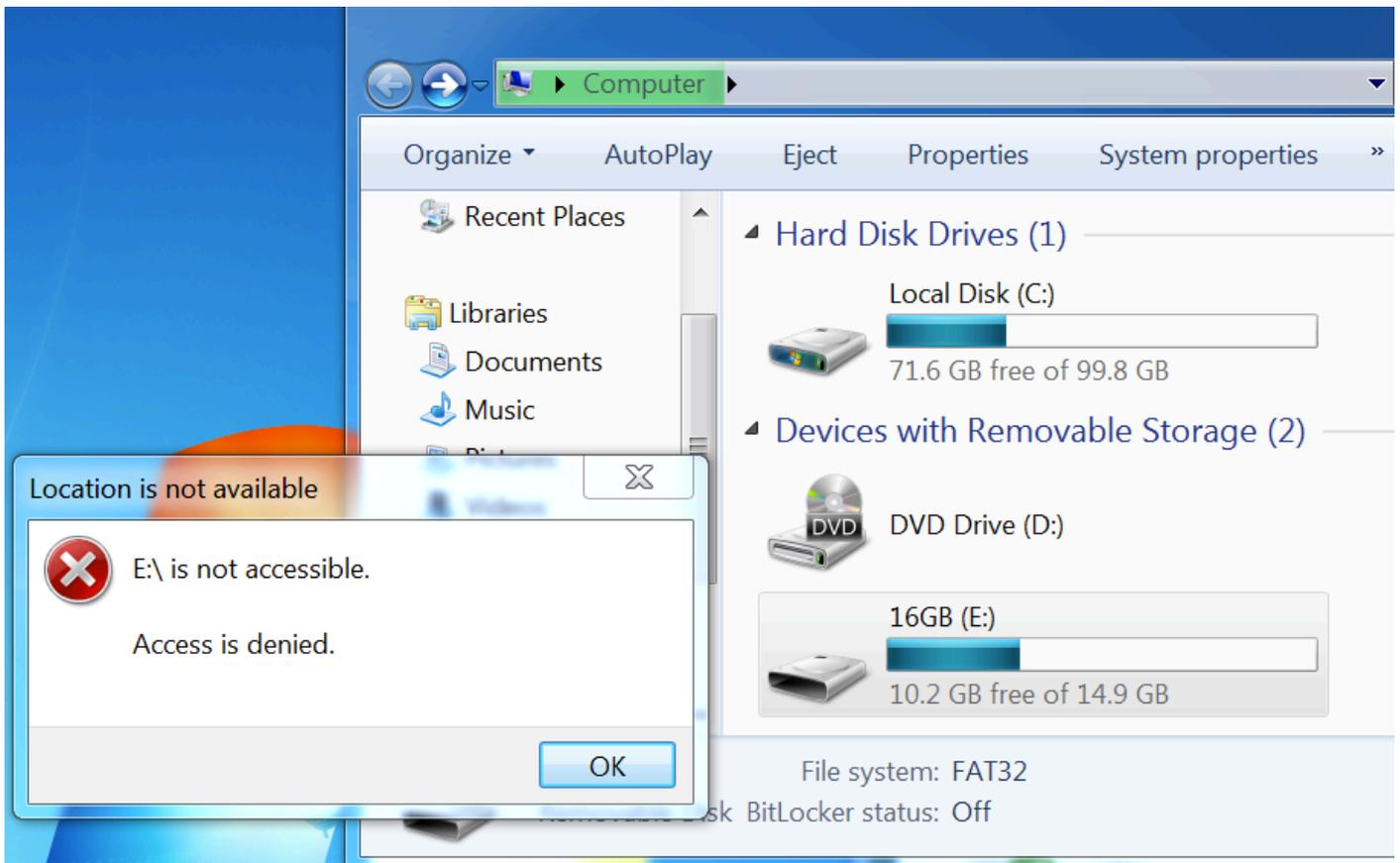
Se necessário, AnyConnect junto com o módulo da postura e da conformidade é atualizado.

Verificação da postura e CoA

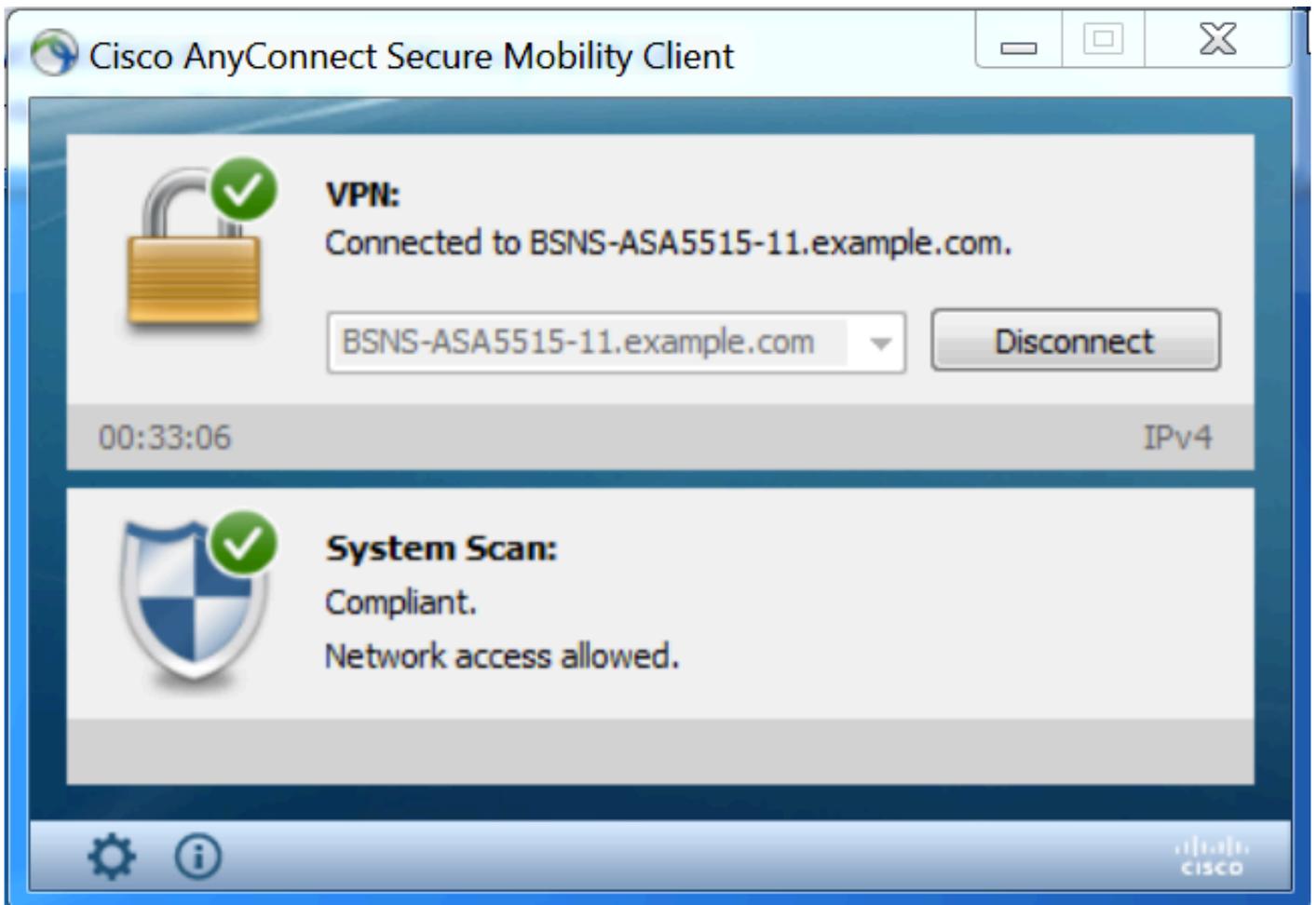
O módulo da postura é executado, descobre ISE (se pôde exigir para ter o registro DNS A para que enroll.cisco.com suceda), transfere e verifica condições da postura, ação nova do dispositivo do bloco USB OPSWAT v4. A mensagem configurada será indicada para o usuário:



Uma vez que a mensagem é confirmada, o dispositivo USB está já não disponível para o usuário:



O ASA remove a reorientação ACL que fornece o acesso direto. AnyConnect relata a conformidade:



Igualmente os relatórios detalhados no ISE podem confirmar que as circunstâncias exigidas estão passadas.

Avaliação da postura pela circunstância:

Report Selector

Posture Assessment by Condition

From 03/11/2016 12:00:00.000 AM to 03/11/2016 04:37:13.253 PM

Logged At	Posture	Identity	Endpoint ID	IP Address	Location	Endpoint OS	Policy	Enforcement Type	Condition Status	Condition name
2016-03-11 16:06:24.974	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:31:53.456	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:26:57.007	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:16:33.483	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check

Avaliação da postura pelo valor-limite:

Report Selector

Posture Assessment by Endpoint

From 03/11/2016 12:00:00.000 AM to 03/11/2016 04:33:39.111 PM

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2016-03-11 16:06:24.974	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint
2016-03-11 11:31:53.456	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint
2016-03-11 11:26:57.007	✓		logoff	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Posture service received a USB-check report from an endpoint
2016-03-11 11:16:33.483	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint

Detalhes de relatório do valor-limite:

Posture More Detail Assessment

Time Range: From 03/11/2016 12:00:00 AM to 03/11/2016 04:34:03.708 PM
 Generated At: 2016-03-11 16:34:03.708

Username: cisco
 Mac Address: 00:0C:29:C9:D9:37
 IP address: 10.48.66.202
 Location: All Locations
 Session ID: 0a3042ca0001d00056e2dce3
 Client Operating System: Windows 7 Ultimate 64-bit
 Client NAC Agent: AnyConnect Posture Agent for Windows 4.3.00520
 PRA Enforcement: 0
 CoA: Received a posture report from an endpoint
 PRA Grace Time: 0
 PRA Interval: 0
 PRA Action: N/A
 User Agreement Status: NotEnabled
 System Name: WIN7-PC
 System Domain: n/a
 System User: Win7
 User Domain: Win7-PC
 AV Installed:
 AS Installed:
 AM Installed: Windows Defender;6.1.7600.16385;1.215.699.0;03/09/2016;

Posture Report
 Posture Status: Compliant
 Logged At: 2016-03-11 16:06:24.974

Posture Policy Details

Policy	Name	Enforcement Type	Status	Passed Conditions	Failed Conditions	Skipped Conditions
Windows 7 USB check	USB_Block	Mandatory		USB_Check		

Troubleshooting

O ISE pode fornecer os detalhes nas circunstâncias de falha, ações deve ser tomado em conformidade.

Referências

- [Como configurar um servidor externo para autorização de usuário de dispositivo de segurança](#)
- [Guia de configuração de CLI para VPN da Cisco ASA Series, 9.1](#)
- [Guia do administrador do Cisco Identity Services Engine, liberação 2.0](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)