Konfigurationsbeispiel für die Integration von AnyConnect 4.0 in ISE Version 1.3

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten **Topologie und Fluss Konfigurieren** WLC ISE Schritt 1: WLC hinzufügen Schritt 2: Konfigurieren des VPN-Profils Schritt 3: Konfigurieren des NAM-Profils Schritt 4: Installieren der Anwendung Schritt 5: Installieren des VPN/NAM-Profils Schritt 6: Konfigurieren der Statusüberprüfung Schritt 7: Konfigurieren von AnyConnect Schritt 8: Client-Bereitstellungsregeln Schritt 9: Autorisierungsprofile Schritt 10: Autorisierungsregeln Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument werden die neuen Funktionen der Cisco Identity Services Engine (ISE) Version 1.3 beschrieben, mit denen Sie mehrere AnyConnect Secure Mobility Client-Module konfigurieren und diese automatisch für das Endgerät bereitstellen können. In diesem Dokument wird die Konfiguration von VPN-, Network Access Manager- (NAM) und Statusmodulen auf der ISE erläutert und an den Benutzer des Unternehmens weitergeleitet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ISE-Bereitstellungen, -Authentifizierung und -Autorisierung
- Konfiguration der Wireless LAN Controller (WLCs)
- Grundlegendes VPN und 802.1x-Wissen

• Konfiguration von VPN- und NAM-Profilen mit AnyConnect-Profil-Editoren

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco WLC 7.6 oder höher
- Cisco ISE Software, Versionen 1.3 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Topologie und Fluss



Hier ist der Ablauf:

Schritt 1: Firmenbenutzer greifen auf Service Set Identifier (SSID) zu: Bereitstellung. 802.1x-

Authentifizierung mit Extensible Authentication Protocol-Protected EAP (EAP-PEAP). Die **Provisioning** Authorization-Regel findet auf der ISE statt, und der Benutzer wird für AnyConnect Provisioning (über das Client Provisioning Portal) umgeleitet. Wenn AnyConnect auf dem Computer nicht erkannt wird, werden alle konfigurierten Module installiert (VPN, NAM, Posture). Zusammen mit diesem Profil wird die Konfiguration für jedes Modul angefordert.

Schritt 2: Nach der Installation von AnyConnect muss der Benutzer den PC neu starten. Nach dem Neustart wird AnyConnect ausgeführt, und die richtige SSID wird gemäß dem konfigurierten NAM-Profil (Secure_Access) automatisch verwendet. EAP-PEAP wird verwendet (z. B. kann auch Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) verwendet werden). Gleichzeitig überprüft das Posture-Modul, ob die Station den Vorgaben entspricht (überprüft, ob eine c:\test.txt-Datei vorhanden ist).

Schritt 3: Wenn der Status der Workstation unbekannt ist (kein Bericht vom Statusmodul), wird er dennoch zur Bereitstellung umgeleitet, da die Regel **Unknown** Authz (Unbekannte Autoren) auf der ISE angetroffen wird. Sobald die Station die Vorgaben erfüllt hat, sendet die ISE eine CoA (Change of Authorization) an den Wireless LAN Controller, was eine erneute Authentifizierung auslöst. Eine zweite Authentifizierung wird durchgeführt, und die **Compliance-**Regel wird auf die ISE angewendet, die dem Benutzer vollständigen Zugriff auf das Netzwerk ermöglicht.

Als Ergebnis wurden dem Benutzer AnyConnect-VPN-, NAM- und Statusmodule bereitgestellt, die einen einheitlichen Netzwerkzugriff ermöglichen. Ähnliche Funktionen können auf der Adaptive Security Appliance (ASA) für den VPN-Zugriff verwendet werden. Derzeit kann die ISE das Gleiche für alle Zugriffsarten mit einem sehr präzisen Ansatz tun.

Diese Funktion ist nicht auf Benutzer in Unternehmen beschränkt, sondern wird meist für diese Benutzergruppe bereitgestellt.

Konfigurieren

WLC

Der WLC ist mit zwei SSIDs konfiguriert:

- Bereitstellung [WPA + WPA2][Auth(802.1X)]. Diese SSID wird für die AnyConnect-Bereitstellung verwendet.
- Secure_access [WPA + WPA2][Auth(802.1X)] Diese SSID wird f
 ür den sicheren Zugriff verwendet, nachdem der Endpunkt mit dem f
 ür diese SSID konfigurierten NAM-Modul bereitgestellt wurde.

ISE

Schritt 1: WLC hinzufügen

Fügen Sie den WLC den Netzwerkgeräten auf der ISE hinzu.

Schritt 2: Konfigurieren des VPN-Profils

Konfigurieren Sie das VPN-Profil mit dem AnyConnect Profile Editor für VPN.

/PN Preferences (Part 1) Preferences (Part 2)	Server List Profile: Untitled				
Backup Servers Certificate Matching	🔒 Server List Entry				
Certificate Enrolment Noble Policy Server List	Host Display Name (required)	asav2	Liker Group	Additional mobile-only settings	Edt
	asav2.example.com		/ TAC		
	Group URL				
	asav2.example.com/TAC				
	Backup Server List			Load Balancing Server List	
				"Always On" is disabled. Load Balancing Fi	elds have been disabled.
	Host Address		Add	Host Address	Add
			Move Up		Delete
			Move Down		
			Delete		
]		
	Primary Protocol		SSL 💌	Automatic SCEP Host	
	Standard Authentication Only	(IOS gateways)	i i i i i i i i i i i i i i i i i i i	CAURL	
	Auth Method During IKE Ne	gotiation	IXE-RSA +	Prompt For Challenge Password	
	DKE Identity			CA Thumbprint	

Für den VPN-Zugriff wurde nur ein Eintrag hinzugefügt. Speichern Sie die XML-Datei in VPN.xml.

Schritt 3: Konfigurieren des NAM-Profils

Konfigurieren Sie das NAM-Profil mit dem AnyConnect Profile Editor für NAM.

tion Policy		Mada Tura
roups Name:	secure_access	Security Leve
Group Membership		Connection Ty
In group:	Local networks 👻	User Auth
 In all groups (Global) 		Credentials
Choose Your Network Media		
Wired (802.3) Network		
Select a wired network	f the endetations will be connection to the network with a traditional	
ethernet cable.	are characteristic connecting to the network more additional	
(a) UE E (violand) Natural		
WI-FI (WIFEIESS) Network	۶	
Select a WiFi network if	the endstations will be connecting to the network via a wireless	
radio connection to an A	ccess Point.	
SSID (max 32 chars):	secure_access	
	Hidden Network	
	Corporate Network	
Association Timeout (see	c) 5	
Common Sottings		
Common Setungs		
Script or application on each u	ser's machine to run when connected.	
	Browse Local Machine	
Connection Timeout (sec.)	40	

Es wurde nur eine SSID konfiguriert: secure_access. Speichern Sie die XML-Datei in NAM.xml.

Schritt 4: Installieren der Anwendung

1. Laden Sie die Anwendung manuell von Cisco.com herunter.

anyconnect-win-4.0.00048-k9.pkganyconnect-win-compliance-3.6.9492.2.pkg

- 2. Navigieren Sie auf der ISE zu **Richtlinien > Ergebnisse > Client Provisioning > Resources**, und fügen Sie Agent Resources from Local Disk hinzu.
- 3. Wählen Sie Cisco Provided Packages (Von Cisco bereitgestellte Pakete) aus, und wählen Sie **anyconnect-win-4.0.0048-k9.pkg aus**:

Check Physicality AnyConnect Uploaded Resources Name Type Version Description AnyConnectDesktopWindows 4 AnyConnectDesktopWin 4.0.48.0 AnyConnect Secure Mobe	Authorization Dictionaries Conditions Results Results Authorization A	Agent Resources From Loc Agent Resources From Loc Agent Resources Fr Category	Clerit Provisioning Trust al Disk > Agent Resources From Local rom Local Disk Cisco Provided Packages • /mnt/crypt/home/mgarcarz	Sec Policy Elements Disk 0 //Downloads/anyconn	nect- <u>Brow</u>	rse
	Coest Provisioning EResources TruciSec		AnyConnect Uploaded Resources Name AnyConnectDesktopWindows 4	Type AngConnectDesktogWin	Version 4.0.48.0	Description AnyConnect Secure Mobility

4. Wiederholen Sie Schritt 4 für das Compliance-Modul.

Schritt 5: Installieren des VPN/NAM-Profils

- 1. Navigieren Sie zu **Richtlinien > Ergebnisse > Client Provisioning > Resources**, und fügen Sie Agent Resources from Local Disk hinzu.
- 2. Wählen Sie vom Kunden erstellte Pakete aus, und geben Sie **AnyConnect Profile ein**. Wählen Sie das zuvor erstellte NAM-Profil (XML-Datei) aus:

🔔 Authentication	 Authorization 	🛃 Profiling	💽 Posture	Client Provisioning	🔂 TrustSec	Policy Elements	
Dictionaries Condi	tions Results						
Results	م ©	Agent Re Agent	category Category Type * Name Description	al Disk > Agent Resources i rom Local Disk Customer Created Packae AnyConnect Profile NAM-Profile /mnt/crypt/tmp/N/	From Local Disk		Browse
		Subm	it Cancel				

3. Wiederholen Sie ähnliche Schritte für das VPN-Profil:

Authentication 💿 Authorization	🔀 Profiling 🛛 👩 Posture	🛃 Client Provisioning 🛛 🔂 TrustSec	Policy Elements
Dictionaries Conditions Res	ults		
Results	Agent Resources From Loc Agent Resources From Loc Category Type * Name Description	al Disk > Agent Resources From Local Disk rom Local Disk Customer Created Packages • @ AnyConnect Profile • VPN-Profile //mnt/crypt/tmp/VPN.xml	Browse
	Submit Cancel		

Schritt 6: Konfigurieren der Statusüberprüfung

NAM- und VPN-Profile müssen extern mit dem AnyConnect-Profil-Editor konfiguriert und in die ISE importiert werden. Der Status ist jedoch vollständig auf der ISE konfiguriert.

Navigieren Sie zu **Richtlinien > Bedingungen > Status > Dateibedingung**.Sie können sehen, dass eine einfache Bedingung für das Vorhandensein einer Datei erstellt wurde. Sie müssen diese Datei haben, um die Richtlinien zu erfüllen, die vom Posture-Modul überprüft wurden:

cisco Identity Services Engine	🏠 Home	Operations 🔻	Policy 🔻	Guest Access 🔻	Administration •
Authentication Authorization Regulte	iling 👩 Posture	🕎 Client Provi	isioning	📑 TrustSec 🛛 🗧	🐴 Policy Elements
Posture F	le Conditions List > file- ile Condition	condition			
	Des	* Name file-cond	dition		
Registry Condition	* F	ile Path ABSOLU	JTE_PATH	▼ C:\test.txt	۲
Application Condition Service Condition	* File O	perator Exists	1011/0	• •	
Compound Condition AV Compound Condition	* Operating	System Window	is All 💠		
AS Compound Condition	Save Reset				
Dictionary Compound Condition					

Diese Bedingung wird für eine Anforderung verwendet:

cisco Identity Services Engine	🏠 Home Operation	is I▼ Policy I▼ GuestAccess	I • Administration I •	
🛓 Authentication 🛛 🧕 Authorization 🔀	Profiling 🛛 🖸 Posture 🔂 Clier	nt Provisioning 🔤 TrustSec	Policy Elements	
Dictionaries Conditions Results				
Results	Bequirements			
٩	Name	Operating Systems	Conditions	Remediation Actions
🌾 🕈 🗄 🔹 🛞 🗸				
Aathentication	FileRequirement	for Windows All	metif file-condition	else Message Text Only
Authorization Profiliog	Any_AV_Installation_Win	for Windows All	metif ANY_av_win_inst	else Message Text Only
 ▼ Posture ▶ = Remediation Actions 	Any_A/_Definition_Win	for Windows All	metif ANY_av_win_def	else Any#vDefRemediationWi n
E Requirements Client Provisioning	Any_AS_installation_Win	for Windows All	metif ANY_as_win_inst	else Message Text Only
 TrustSec 	Any_AS_Definition_Win	for Windows All	metif ANY_as_win_def	else AnyASDefRemediationWi n
	Any_A/_Installation_Mac	for Mac OSX.	metif ANY_av_mac_inst	else Message Text Only
	Any_A/_Definition_Mac	for Mac OSX.	metif ANY_av_mac_def	else AnyAVDefRemediationMa c
	Any_AS_installation_Mac	for Mac OSX	metif ANY_as_mac_inst	else Message Text Only
:	Any_AS_Definition_Mac	for Mac OSX	metif ANY_as_mac_def	else AnyASDerRemediationMa c

Die Anforderung wird in der Statusrichtlinie für Microsoft Windows-Systeme verwendet:

cisco Identity Ser	rvices Engine		🏠 Home	Opera	tions 🔻	Policy •	Guest Access	۲	Administration	,	
🚉 Authentication	 Authorization 	🔀 Profiling	😿 Posture		Client Provi	sioning	📑 TrustSec	- 3	Policy Elements		
Posture Policy Define the Posture Policy	by configuring rules base	ad on operatin	g system and/or other o	condition	18.						
Status Rule Na	ame		Identity Groups	(Operating S	Systems	Other Con	dition	s		Requirements
🖌 File		r.	Any	and 1	Vindows A	I				then	FileRequirement

Weitere Informationen zur Statuskonfiguration finden Sie <u>im Cisco ISE-Konfigurationshandbuch</u> unter <u>Statusservices</u>.

Wenn die Status-Richtlinie bereit ist, ist es an der Zeit, die Status-Agent-Konfiguration hinzuzufügen.

- 1. Navigieren Sie zu **Richtlinien > Ergebnisse > Client Provisioning > Resources,** und fügen Sie Network Admission Control (NAC) Agent oder AnyConnect Agent Posture Profile hinzu.
- 2. Wählen Sie AnyConnect aus (ein neues Statusmodul aus ISE Version 1.3 wurde anstelle des alten NAC Agent verwendet):

ዿ Authentication	👩 Auth	orization	<u>s</u> 1	Profiling	💽 Posture	🔊 Clie	nt Provisioning
Dictionaries	Conditions	Results					
Results				ISE Posture	Agent Profile S	ettings > N	ew Profile
(م ش)	Posture Age	ent Profile Settir	ngs	
Authentication	2	ini V		* Name:	ISEPosture]
 Authorization Profiling 				Description			
Posture Client Provisi	oning						
E Resources	g			Agent Beha	wior		

3. Vergessen Sie nicht, im Abschnitt Posture Protocol * hinzuzufügen*, damit der Agent eine Verbindung zu allen Servern herstellen kann.

Posture Protocol		
Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all

4. Wenn das Feld Servername-Regeln leer bleibt, speichert die ISE keine Einstellungen und meldet diesen Fehler:

Server name rules: valid value is required

Schritt 7: Konfigurieren von AnyConnect

In dieser Phase wurden alle Anwendungen (AnyConnect) und die Profilkonfiguration für alle Module (VPN, NAM und Status) konfiguriert. Es ist an der Zeit, sie zusammenzubinden.

- 1. Navigieren Sie zu **Richtlinien > Ergebnisse > Client Provisioning > Resources**, und fügen Sie AnyConnect Configuration hinzu.
- 2. Konfigurieren Sie den Namen, und wählen Sie das Compliance-Modul und alle erforderlichen AnyConnect-Module (VPN, NAM und Status) aus.
- 3. Wählen Sie in Profile Selection (Profilauswahl) das Profil aus, das zuvor für jedes Modul konfiguriert wurde.

🔔 Authentication 🛛 🧕 Authorization	🔀 Profiling 🛛 🧑 Posture 🛛 🙀 Client Provisio	oning 📄 TrustSec 🛛 🐴 Policy Elements
Dictionaries Conditions Results		
Results	AnyConnect Configuration > AnyConnect Con	nfiguration
Authentication Authorization	* Select AnyConnect Package:	AnyConnectDesktopWindows 4.0.48.0 *
Profiling Posture	* Configuration Name:	AnyConnect Configuration
Client Provisioning El Resources	Description:	
 TrustSec 	Description	Value
	* Compliance Module	AnyConnectComplianceModuleWindows 3.6.5 +
	AnyConnect Module Selection	
	ISE Posture	
	VPN	
	Network Access Manager	
	Web Security	
	ASA Posture	
	Start Before Logon	
	Diagnostic and Reporting Tool	
	Profile Selection	
	* ISE Posture	ISEPosture 👻
	VPN	VPN-Profile *
	Network Access Manager	NAM-Profile *
	Web Security	
	Customer Feedback	Ţ

4. Das VPN-Modul ist für die korrekte Funktion aller anderen Module obligatorisch. Auch wenn das VPN-Modul nicht für die Installation ausgewählt ist, wird es auf den Client übertragen und installiert. Wenn Sie kein VPN verwenden möchten, können Sie ein spezielles VPN-Profil konfigurieren, das die Benutzeroberfläche für das VPN-Modul verbirgt. Diese Posten sollten der Datei VPN.xml hinzugefügt werden:

<ClientInitialization>

5. Diese Art von Profil wird auch installiert, wenn Sie Setup.exe aus dem ISO-Paket (anyconnect-win-3.1.06073-pre-deploy-k9.iso) verwenden. Anschließend wird das VPNDisable_ServiceProfile.xml-Profil für VPN zusammen mit der Konfiguration installiert, wodurch die Benutzeroberfläche für das VPN-Modul deaktiviert wird. Auf die in Schritt 7 erstellte AnyConnect-Konfiguration sollte in den Client-Bereitstellungsregeln verwiesen werden:

ahaha cisco li	dentity Services F	ngine										
cisco in	senary services i	- Ingine		🕜 Н	ome Op	arations 🛛 🔻	Polic	y 🔻	Guest Access	 Admini 	stration	
🔔 Authen	tication 🧕 Au	thorization [🖌 Profiling	💌 Posti	ure 🗾 🖬	Client Pro	visioning		🚊 TrustSec	🐥 Policy E	lements	
Client Pro	ovisioning Polic	cy										
Define the Cli For Agent Cor For Native Su	ent Provisioning Poli Ifiguration: version of pplicant Configuration	cy to determine wh: (agent, agent profile n: wizard profile and	at users will recei e, agent complian s/or wizard. Drag a	re upon lo ce modul and drop r	gin and use e, and/or age ules to chan	r session in ant customia ge the order	itiation: zation pao r.	kage.				
¥												
	Rule Name		Identity Groups		Operating S	lystems		Other	Conditions			Results
	AnyconnectWin	If	Any	and	Windows Al	I	and	Condit	ion(s)		then	AnyConnect Configuration

Client-Bereitstellungsregeln legen fest, welche Anwendung an den Client weitergeleitet wird. Hier ist nur eine Regel erforderlich, die auf die in Schritt 7 erstellte Konfiguration verweist. Auf diese Weise verwenden alle Microsoft Windows-Endpunkte, die für die Client-Bereitstellung umgeleitet werden, die AnyConnect-Konfiguration mit allen Modulen und Profilen.

Schritt 9: Autorisierungsprofile

Das Autorisierungsprofil für die Client-Bereitstellung muss erstellt werden. Das Standard-Client Provisioning Portal wird verwendet:

alah				
cisco Identity Services Engine	🏠 Home	Operations Policy	Guest Access 🔻	Administration •
🛃 Authentication 🛛 🧔 Authorization 🔀	Profiling 👩 Posture	👸 Client Provisioning	📑 TrustSec 🛛 📑	Policy Elements
Dictionaries Conditions Results				
Results	Authorization Profiles > Guer Authorization Profile *Name GuestPr Description * Access Type ACCESS Service Template	ACCEPT *		
Q LimitedAccess	▼ Common Tasks			
Non_Cisco_P_Phones SemitAccess Downloadable ACLs	Web Redirection (CWA, MI	DM, NSP, CPP)		
Inline Posture Node Profiles Profiling	Client Provisioning (Pos	ture) 🔻 ACL GuestRedire	ect	Value Client Provisioning Portal +

Dieses Profil erzwingt die Umleitung der Benutzer zur Bereitstellung an das Standard-Client-Bereitstellungsportal. Dieses Portal evaluiert die Client Provisioning Policy (Regeln, die in Schritt 8 erstellt wurden). Autorisierungsprofile sind die Ergebnisse der in Schritt 10 konfigurierten Autorisierungsregeln.

GuestRedirect Access Control List (ACL) ist der Name der auf dem WLC definierten ACL. Diese ACL legt fest, welcher Datenverkehr an die ISE umgeleitet werden soll. Weitere Informationen finden Sie unter Konfigurationsbeispiel für die zentrale Webauthentifizierung mit einem Switch und der Identity Services Engine.

Es gibt auch ein weiteres Autorisierungsprofil, das den begrenzten Netzwerkzugriff (DACL) für nicht konforme Benutzer (LimitedAccess genannt) bereitstellt.

Schritt 10: Autorisierungsregeln

Alle werden in vier Autorisierungsregeln zusammengefasst:

abab								
cisco Ide	entity Services Engine		🟠 Home	Operations •	Policy 🔻	Guest Access	▼ Ac	Iministration 🔻
🚨 Authentic	ation 🦲 Authorization	🛃 Profiling	💽 Posture	😡 Client Provis	sioning	🚉 TrustSec	🐥 Po	licy Elements
Authorizati	ion Policy							
Define the Author For Policy Expor	orization Policy by configuring rules t go to Administration > System	: based on identity n > Backup & R	groups and/or othe estore > Policy E	r conditions. Drag a xport Page	ind drop rule	s to change the orde	er.	
First Matcheo	d Rule Applies 🔹							
Exception:	s (0)							
Standard								
Status	Rule Name	C	onditions (identity gr	oups and other con	ditions)			Permissions
	Compliant	if <mark>(R</mark> a Se	idius:Called-Station ssion:PostureStatus	-ID CONTAINS sec EQUALS Complia	ure_access nt)	AND	then	PermitAccess
	NonCompliant	if <mark>(R</mark> a Se	dius:Called-Station ssion:PostureStatus	-ID CONTAINS sec EQUALS NonCom	ure_access pliant)	AND	then	LimitedAccess
	Unknown	if <mark>(R</mark> a Se	adius:Called-Station ssion:PostureStatus	-ID CONTAINS sec EQUALS Unknown	ure_access	AND	then	GuestProvisioning
	Provisioning	if <mark>(R</mark> a Sei	adius:Called-Station ssion:PostureStatus	-ID CONTAINS prov EQUALS Unknown	isioning ANG 1)		then	GuestProvisioning

Zuerst stellen Sie eine Verbindung zum Provisioning SSID her und werden zur Bereitstellung an ein Standard-Client Provisioning Portal (Regel namens Provisioning) umgeleitet. Wenn Sie eine Verbindung mit der **Secure_Access** SSID herstellen, wird die Bereitstellung trotzdem umgeleitet, wenn kein Bericht des Statusmoduls von der ISE empfangen wird (Regel mit dem Namen Unknown). Sobald der Endpunkt vollständig kompatibel ist, wird der vollständige Zugriff gewährt (Regelname erfüllt). Wenn der Endpunkt als nicht konform gemeldet wird, verfügt er über eingeschränkten Netzwerkzugriff (Regel heißt "NonCompliant").

Überprüfen

Sie ordnen sich der Provisioning SSID zu, versuchen, auf eine beliebige Webseite zuzugreifen, und werden an das Client Provisioning Portal umgeleitet:



Da AnyConnect nicht erkannt wird, werden Sie zur Installation aufgefordert:

Device Security Check

Your computer requires security software to be installed before you can connect to the network.



Unable to detect AnyConnect Posture Agent

Eine kleine Anwendung namens Network Setup Assistant, die für den gesamten Installationsprozess verantwortlich ist, wird heruntergeladen. Beachten Sie, dass es sich in Version 1.2 von dem Network Setup Assistant unterscheidet.



Alle Module (VPN, NAM und Status) werden installiert und konfiguriert. Sie müssen Ihren Computer neu starten:



Nach dem Neustart wird AnyConnect automatisch ausgeführt, und NAM versucht, eine Verbindung zur sicheren_Zugriff-SSID herzustellen (entsprechend dem konfigurierten Profil). Beachten Sie, dass das VPN-Profil korrekt installiert ist (ASAV2-Eintrag für VPN):

Cisco AnyConnect secure_access	S Cisco AnyConnect Secure Mobility Client
Please enter your username and password for the network: secure_access Username:	VPN: Verify your network connection.
Show Password	No Network Connectivity
OK Cancel	Network: Authenticating secure_access
	System Scan: Limited or no connectivity.

Nach der Authentifizierung lädt AnyConnect Aktualisierungen sowie Statusregeln herunter, für die eine Überprüfung durchgeführt wird:

🕙 Cisco AnyCo	nnect Secure Mobility Client	- • •
	VPN: Ready to connect. asav2	✓ Connect
	Network: Connected (10.221.0.250) secure_access	- III - III
	System Scan: Checking requirement 1 of 1.	
\$ (i)		a juaju cisco

In dieser Phase kann der Zugriff weiterhin eingeschränkt sein (Sie sehen die Unknown Authorization-Regel auf der ISE). Sobald die Station den Vorgaben entspricht, wird sie vom Posture-Modul gemeldet:

🕤 Cisco AnyCo	nnect Secure Mobility Client	
	VPN: Ready to connect. asav2	Connect
	Network: Connected (10.221.0.250) secure_access	
	System Scan: Compliant. Network access allowed.	
\$ (i)		altalia cisco

Die Details können ebenfalls überprüft werden (die FileRequirement-Anweisung ist erfüllt):

Sisco AnyConnect Secure Mobility Client		- • •
cisco AnyConne	ct Secure Mobility Client	0
Status Overview	System Scan	
VPN	Preferences Statistics Security Products Scan Summary	Message History
Network	Updates	Status
System Scan >	1 S FileRequirement	Done

Der Nachrichtenverlauf zeigt detaillierte Schritte:

```
9:18:38 AM The AnyConnect Downloader is performing update checks...
9:18:38 AM Checking for profile updates...
9:18:38 AM Checking for product updates...
```

9:18:38 AM Checking for customization updates... 9:18:38 AM Performing any required updates... 9:18:38 AM The AnyConnect Downloader updates have been completed. 9:18:38 AM Update complete. 9:18:38 AM Scanning system ... 9:18:40 AM Checking requirement 1 of 1. 9:18:40 AM Updating network settings ... 9:18:48 AM Compliant.

Der erfolgreiche Bericht wird an die ISE gesendet, was den Autorisierungswechsel auslöst. Bei der zweiten Authentifizierung wird die Compliance-Regel beachtet, und der vollständige Netzwerkzugriff wird gewährt. Wenn der Statusbericht gesendet wird, während er weiterhin der Provisioning SSID zugeordnet ist, werden diese Protokolle auf der ISE angezeigt:

oliside CISCO	dentity Ser	vices Engine			A Home C	perations * Policy *	Quest Access • Ad	Iministration •		Lances We	und X mers summ rudow
💽 Auftrantiscations 👖 Reports 🙀 Endpoint Protection Service 💊 Troubleshoot											
Misconfigured Supplicants (2) Misconfigured Network Devices (2) PADIUS Drops (2) Client Stopped Responding (2) 0 0 0 1										ed Responding (1) 1	
1 Shi	w Live Sessions	Add or Re	move Co	dumns 💌 🏀 I	Refresh 👩 Reset Re	peat Counts				Refresh Ever	y1 minute * Show Latest 20
Time		Status AJ • Det.	. P	identity ®	Endpoint ID	Authorization Policy ®	Authorization Profiles	Network Device	Posture Status	Server ®	Event 2
2014-1	1.16 09.32.07.	. 0 . 6	0	cisco	C0:44.00:15:64.DC				Compliant	ise13	Session State is Started
2014-1	1-16 09:32:07.	- 🖬 🔒		cisco	C0:44.00:15:64.0C	Default >> Compliant	PermitAccess	WLC1	Compliant	isel3	Authentication succeeded
2014-1	1.16 09:32:07.	. 🖬 🧿			C0:44:00:15:64:DC			WLC1	Compliant	ise13	Dynamic Authorization succeeded
2014-1	1-16 09:31:35.	. 0 .		admin	C0:44:00:15:64:DC			WLC1		ise13	Authentication failed
2014-1	1-16 09:29:34.	. 🖬 💊		cisco	C0:44.00:15:6A.DC	Default >> Provisioning	GuestProvisioning	WLC1	Pending	ise13	Authentication succeeded

Der Statusbericht zeigt Folgendes an:

allalla							Louise Marsing	A 1 MIT 1	aleas y Legent y Poellack D
cisco Identity Services Engine	🙊 Home	Operations	 Policy I 	• QuestAcces	s I • Administratio	1.			Setup
Authentications Reports 20	ndpoint Protection Service	Troublesho	et.						
Report Selector	Posture Detail Assessm	unt .							👷 Favorite 🛛 🚇 Export
Favorites									Generated at 2014
ISE Reports	From 11/16/2014 12:00:00 AM	lo 11/16/2014	09.27:56 AM						Page of 3 in Resolution
 Auth Services Status 	Logged At St	tus Detail	PRA	identity	Endpoint ID	P Address	Endpoint OS	Agent	Message
ll rapada	2014-11-16 09:23:25.8	e 6	NIA	cisco	C0.44.00.15.6A.D	10.221.0.250	Windows 7 Utsmate 64-64	AnyConnect	Received a posture report from an endpoint
 Depityment Status 12 reports 	2014-11-16 09-18:42-2	0	NIA	disco	C0-44-00-15-64-D	10.221.0.250	Windows 7 Ultimate 64-64	AnyConnect	Received a posture report from an endpoint
+ Endpoints and Users	2014-11-16-09-16-59-6	0	NUA	cisco	C0-44-00-15-64-D	10.221.0.250	Windows 7 Utimate 64-64	AnyConnect	Received a posture report from an endpoint
Client Provisioning	2014-11-16 09:15:17.4	a 🔉	NA	disce	C0.44.00.15.6A.D	10.221.0.250	Windows 7 Utimate 64-bit	AnyConnect	Received a posture report from an endpoint
Current Active Sessions									
Endpoint Protection Senice Audit									
External Hobile Device Management									
Posture Detail Assessment ¹ ²⁷ Hiters • * Time Range Today •									

Detaillierte Berichte zeigen die erfüllte FileRequirement an:

Posture More Detail Assessment

Time Range: From 11/16/2014 12:00:00 AM to 11/16/2014 09:28:48 AM Generated At: 2014-11-16 09:28:48.404

Client Details						
Username:	cisco					
Mac Address:	C0:4A:0	0:15:6A:DC				
IP address:	10.221.	0.250				
Session ID:	0a3e47	35000002a354685ee	2			
Client Operating System	m: Window	s 7 Ultimate 64-bit				
Client NAC Agent:	AnyCon	nect Posture Agent fo	r Window	s 4.0.00048		
PRA Enforcement:	0					
CoA:	Receive	d a posture report fro	m an end	point		
PRA Grace Time:	0					
PRA Interval:	0					
PRA Action:	N/A					
User Agreement Statu	s: NotEnal	led				
System Name:	ADMIN-	°C				
System Domain:	n/a					
System User:	admin					
User Domain:	admin-F	C				
AV Installed:						
AS Installed:	Window	s Defender;6.1.7600.	16385;1.	147.1924.0;04/16	/2013;	
Posture Report						
Posture Status:	Complia	nt				
Logged At:	2014-11	-16 09:23:25.873				
Posture Policy Details						
Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
File	FileRequiremen	t Mandatory		file-condition		

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- <u>Statusservices im Cisco ISE-Konfigurationsleitfaden</u>
- <u>Cisco ISE 1.3 Administratorhandbuch</u>
- Technischer Support und Dokumentation Cisco Systems