Integration von Duo SAML SSO mit AnyConnect Secure Remote Access mit ISE-Status

Inhalt

Einleitung
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
Konfigurieren
<u>Netzwerkdiagramm</u>
Datenverkehrsfluss
Konfigurationen
- Duo Admin-Portal-Konfiguration
- Duo Access Gateway (DAG)-Konfiguration
-ASA-Konfiguration
-ISE-Konfiguration
Überprüfung
Benutzerfreundlichkeit
Fehlerbehebung
Zugehörige Informationen

Einleitung

In diesem Dokument wird ein Konfigurationsbeispiel für die Integration von Duo SAML SSO mit Adaptive Security Appliance (ASA) Cisco AnyConnect Secure Mobility Client für eine detaillierte Statusüberprüfung mithilfe der Cisco ISE beschrieben. Duo SAML SSO wird mithilfe von Duo Access Gateway (DAG) implementiert, das zur erstmaligen Benutzerauthentifizierung mit dem Active Directory kommuniziert und dann zur mehrstufigen Authentifizierung mit Duo Security (Cloud) kommuniziert. Die Cisco ISE wird als Autorisierungsserver für die Endpunktverifizierung mittels Statusüberprüfung verwendet.

Beitrag von Dinesh Moudgil und Pulkit Saxena, Cisco HTTS Engineer.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die ASA voll funktionsfähig und so konfiguriert ist, dass mit dem Cisco Adaptive Security Device Manager (ASDM) oder der Befehlszeilenschnittstelle (Command Line Interface, kurz "CLI") Konfigurationsänderungen möglich sind.

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlagen zu Duo Access Gateway und Duo Security
- Grundkenntnisse der VPN-Konfiguration für Remote-Zugriff auf der ASA
- Grundkenntnisse der ISE und Statusservices

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco Adaptive Security Appliance-Software Version 9.12(3)12
- Duo Access-Gateway
- Duo Security
- · Cisco Identity Services Engine Version 2.6 und höher
- Microsoft Windows 10 mit AnyConnect Version 4.8.03052

Hinweis: Für jeden in dieser Implementierung verwendeten Embedded Browser von AnyConnect ist die ASA Version 9.7(1)24, 9.8(2)28, 9.9(2)1 oder eine höhere Version jeder Version sowie die AnyConnect-Version 4.6 oder höher erforderlich.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



Datenverkehrsfluss

- 1. AnyConnect-Client initiiert eine SSL VPN-Verbindung zur Cisco ASA
- Cisco ASA, die f
 ür die prim
 äre Authentifizierung mit Duo Access Gateway (DAG) konfiguriert ist, leitet den eingebetteten Browser in Anyconnect Client zur SAML-Authentifizierung an DAG um
- 3. AnyConnect-Client wird auf Duo Access Gateway umgeleitet
- 4. Sobald der AnyConnect-Client die Anmeldeinformationen eingegeben hat, wird eine SAML-Authentifizierungsanforderung erstellt und von Cisco ASA an Duo Access Gateway ausgegeben
- 5. Duo Access Gateway nutzt die Integration mit Active Directory vor Ort, um die primäre Authentifizierung für den AnyConnect-Client durchzuführen
- 6. Sobald die primäre Authentifizierung erfolgreich ist, sendet das Duo Access Gateway über den TCP-Port 443 eine Anforderung an Duo Security, um die Zwei-Faktor-Authentifizierung zu starten.
- 7. Der AnyConnect-Client präsentiert sich mit "Duo Interactive Prompt" und der Benutzer vollendet Duo Zwei-Faktor-Authentifizierung mit seiner bevorzugten Methode (Push oder Passcode)
- 8. Duo Security erhält eine Authentifizierungsantwort und sendet die Informationen an das Duo Access Gateway
- 9. Auf Basis der Authentifizierungsantwort erstellt Duo Access Gateway eine SAML-Authentifizierungsantwort, die eine SAML-Assertion enthält und auf den AnyConnect-Client reagiert

- 10. AnyConnect-Client authentifiziert erfolgreich SSL VPN-Verbindungen mit Cisco ASA
- 11. Nach erfolgreicher Authentifizierung sendet die Cisco ASA eine Autorisierungsanfrage an die Cisco ISE

Hinweis: Cisco ISE ist nur für die Autorisierung konfiguriert, da Duo Access Gateway die erforderliche Authentifizierung bereitstellt.

- 12. Die Cisco ISE verarbeitet die Autorisierungsanfrage und gibt, da der Status des Clients "Unbekannt" lautet, eine Statusumleitung mit eingeschränktem Zugriff auf den AnyConnect-Client über die Cisco ASA zurück.
- 13. Wenn der Anyconnect-Client über kein Compliance-Modul verfügt, wird er aufgefordert, das Modul herunterzuladen, um die Statusüberprüfung fortzusetzen.
- 14. Wenn der AnyConnect-Client über ein Compliance-Modul verfügt, stellt er eine TLS-Verbindung mit der Cisco ASA her, und der Statusfluss beginnt
- 15. Abhängig von den auf der ISE konfigurierten Statusbedingungen werden Statusüberprüfungen durchgeführt, und die Details werden vom AnyConnect-Client an die Cisco ISE gesendet.
- 16. Wenn sich der Status des Clients von Unbekannt zu Konformität ändert, wird von der Cisco ISE eine Anforderung zur Autorisierung (Change of Authorization, CoA) an die Cisco ASA gesendet, um dem Client den vollen Zugriff zu gewähren. Das VPN ist dann vollständig eingerichtet.

Konfigurationen

- Duo Admin-Portal-Konfiguration

Konfigurieren Sie in diesem Abschnitt die ASA-Anwendung auf dem Duo-Administratorportal.

1. Melden Sie sich bei "Duo Admin Portal" an, navigieren Sie zu "Applications > Protect an Application" (Anwendungen > Schutz einer Anwendung), und suchen Sie nach "ASA" mit dem Schutztyp "2FA with Duo Access Gateway, self-hosted" (2FA mit Duo Access Gateway, selbst gehostet). Klicken Sie ganz rechts auf "Schützen", um die Cisco ASA zu konfigurieren.

	admin-77d04ebc.duosecurity.com	m/applications/protect/types				☆	D
lisc	Cisco Study 🗎 Cisco Tools	Mix SourceFire VPN AAA AAA	E IFT 6.7				
	D II O	Q Search for users, groups, applications, or devi	Ces	0	Cisco ID: 2010-1403-48	ciscoduoblr 🗸	
	Dashboard	Dashboard > Applications > Protect an Application)				
	Device Insight	Drote et en Annlie etie					
	Policies	Protect an Applicatio	on				ì
	Applications	(ASA)					J
	Protect an Application	Application	2FA	Single Sign-On (if available)	Documentation	Action	
	Single Sign-On						
	Users	asana Asana	2FA	Duo Access Gateway (self-hosted)	Documentation ⊡*	Protect	
	Groups						
	Endpoints	Cisco ASA	2FA	Duo Access Gateway (self-hosted)	Documentation 🗗	Protect	٦
	2FA Devices	cisco)		J
	Administrators	allalla se sec	254	Single Sign-On (bosted by Duo)			
	Reports	CISCO Cisco ASA	254	Single Sign-On (IDSted by Dub)	Documentation C	Configure	

2. Konfigurieren Sie unter "Service Provider" die folgenden Attribute für die geschützte Anwendung ASA.

Basis-URL	firebird.cisco.com
Tunnelgruppe	TG_SAML
Mail-Attribut	sAMAccountName, E-Mail

Klicken Sie unten auf der Seite auf "Speichern"

Device Insight	Cisco ASA - Duo Access Gateway			
Policies				
Applications	Configure Cisco ASA			
Protect an Application				
Single Sign-On	To set up this application, in	nstall the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions [2]		
Users	Next step: Download your o	configuration file		
Groups				
Endpoints	Service Provider			
2FA Devices				
Administrators	Base URL	firebird.cisco.com		
Reports		Enter the Cisco ASA Base URL.		
Settings				
Billing	Tunnel Group	TG_SAML		
Dining		Enter the Tunnel Group you are protecting with SSO.		
Need Help?				
Chat with Tech Support 대	Custom attributes	Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.		
Email Support				
Call us at 1-855-386-2884				
Account ID 2010-1403-48	Mail attribute	sAMAccountName,mail		
Deployment ID DUO57 대		The attribute containing the email address of the user.		
Helpful Links				
Documentation		Save Configuration		

In diesem Dokument werden für die restliche Konfiguration Standardparameter verwendet. Sie können jedoch entsprechend den Anforderungen des Kunden festgelegt werden. Zu diesem Zeitpunkt können zusätzliche Einstellungen für die neue SAML-Anwendung angepasst werden, z. B. das Ändern des Anwendungsnamens vom Standardwert, das Aktivieren der Self-Service-Funktion oder das Zuweisen einer Gruppenrichtlinie.

3. Klicken Sie auf den Link "Download your configuration file" (Konfigurationsdatei herunterladen), um die Einstellungen der Cisco ASA-Anwendung (als JSON-Datei) abzurufen. Diese Datei wird in späteren Schritten auf das Duo Access Gateway hochgeladen.

Device Insight	Cisco ASA - Duo Access Gateway Authentication Log			e Application
Policies				
Applications	Configure Cisco ASA			Secret Key
Protect an Application	.			
Single Sign-On	To set up this application, ins	stall the Duo Access Gateway and then configure your service provider. View Cisco ASA	SAML SSO instructions	
Users	Next step: Download your co	ntiguration file		
Groups				
Endpoints	Service Provider			
2FA Devices				
Administrators	Base URL	firebird.cisco.com		
Reports		Enter the Cisco ASA Base URL.		
Settinge				
Dilling	Tunnel Group	TG_SAML		
Billing		Enter the Tunnel Group you are protecting with SSO.		
Need Help?				
Chat with Tech Support 더	Custom attributes	✓ Use this setting if your Duo Access Gateway authentication source uses non-star	dard attribute names.	
Email Support Call us at 1-855-386-2884				
Account ID	Mail attribute	sAMAccountName.mail		
2010-1403-48				
Deployment ID DUO57 Cf		The attribute containing the email address of the user.		
Helpful Links				
Documentation		Save Configuration		

4. Unter "Dashboard > Anwendungen" sieht die neu erstellte ASA-Anwendung wie in der Abbildung unten dargestellt aus:

dmin-77d04ebc.duosecurity.com/applications							
🗎 Cisco Study 🗎 Cisco Tools	Mix 🗃 SourceFire 🗎 VPN 🗎 AAA	🗎 ASA 📋 IFT 6.7					
DUO	Q. Search for users, groups, applications,	or devices		G Cisco ID: 2010-1403-48	ciscoduoblr	~	
Dashboard	Dashboard > Applications						
Device Insight							
Policies	Applications			SSO Setup Guide 🖆 Protect a	n Application		
Applications						_	
Protect an Application				Export V Q Search			
Single Sign-On							
Users	Name 🔺	Туре	Application Policy	Group Policies			
Groups	Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway					
Endpoints							
2FA Devices	1 total						

5. Navigieren Sie zu "Benutzer > Benutzer hinzufügen", wie in der Abbildung dargestellt:

Erstellen Sie einen Benutzer namens "duouser", der für die AnyConnect Remote Access-Authentifizierung verwendet werden soll, und aktivieren Sie Duo Mobile auf dem Endbenutzergerät.



Um die Telefonnummer hinzuzufügen, wie im Bild gezeigt, wählen Sie die Option "Telefon hinzufügen".



Aktivieren Sie "Duo Mobile" für den jeweiligen Benutzer



Hinweis: Stellen Sie sicher, dass "Duo Mobile" auf dem Endbenutzergerät installiert ist. <u>Manuelle Installation der Duo Anwendung für IOS Geräte</u> <u>Manuelle Installation der Duo Anwendung für Android Geräte</u>

Wählen Sie "Duo-Aktivierungscode generieren" wie im Bild gezeigt:

DUO	Q Search for users, groups, applications, or devices Ciscoduoblr V
Dashboard	Dashboard > Phone: Activate Duo Mobile
Device Insight	Activate Due Mahila
Policies	Activate Duo Mobile
Applications	This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their
Users	mobile device or authenticate via Duo Push.
Groups	Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.
Endpoints	
2FA Devices	Phone
Phones	
Hardware Tokens	Expiration 24 hours v after generation
WebAuthn & U2F	
Administrators	Generate Duo Mobile Activation Code
Reports	
Settings	

Wählen Sie "Send Instructions by SMS" (Anweisungen per SMS senden) wie im Bild gezeigt:



Klicken Sie auf den Link in der SMS, und die Duo App wird mit dem Benutzerkonto im Abschnitt "Geräteinformationen" verknüpft, wie im Bild gezeigt:



- Duo Access Gateway (DAG)-Konfiguration

1. Bereitstellung von Duo Access Gateway (DAG) auf einem Server in Ihrem Netzwerk

Hinweis: Befolgen Sie zur Bereitstellung die folgenden Dokumente:

Duo Access Gateway für Linux https://duo.com/docs/dag-linux

Duo Access Gateway für Windows https://duo.com/docs/dag-windows

- 2. Navigieren Sie auf der Startseite von Duo Access Gateway zu "Authentication Source"
- 3. Geben Sie unter "Quellen konfigurieren" die folgenden Attribute für Ihr Active Directory ein, und klicken Sie auf "Einstellungen speichern".

Configure Sources

nfigure authenticatior	n source settings below. Changes made to non-active authentication sources will take effect when made active.
Source type	Active Directory Specify the authentication source to configure.
Status:	 ◇ LDAP Bind Succeeded ◇ Idap://10.197.243.110
Server	10.197. 389 Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separated for failover functionality. For example: ad1.server.com, ad2.server.com, 10.1.10.150
Transport type	CLEAR LDAPS STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.
Attributes	SAMAccountName,mail Specify attributes to retrieve from the AD server. For example: sAMAccountName,mail.
Search base	CN=Users,DC=dmoudgil,DC=local
Search attributes	SAMAccountName Specify attributes the username should match against. For example: sAMAccountName,mail.
Search username	iseadmin The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only access
Search password	••••• The password corresponding to the search username specified above.
	Save Settings

4. Wählen Sie unter "Set Active Source" den Quelltyp als "Active Directory" aus, und klicken Sie auf "Set Active Source".

:	Set Active Source	
	Specify the source that e	end-users will use for primary authentication.
Source type		Active Directory
		Set Active Source

5. Navigieren Sie zu "Applications" (Anwendungen hinzufügen), und laden Sie im Untermenü "Add Application" (Anwendung hinzufügen) die JSON-Datei hoch, die Sie von der Duo Admin Console im Abschnitt "Configuration file" (Konfigurationsdatei) heruntergeladen haben. Die entsprechende JSON-Datei wurde in Schritt 3 unter Duo Admin Portal Configuration heruntergeladen.

Applications

Add Application

Create a SAML application	Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here.		
Configuration file	Browse Cisco ASA - Duo Access Gateway.json		
	Upload		

6. Sobald die Anwendung erfolgreich hinzugefügt wurde, wird sie im Untermenü "Anwendungen" angezeigt.

Applications					
Name	Туре	Logo			
Cisco ASA - Duo Access Gateway	Cisco ASA	altatu cisco	Delete		

- 7. Laden Sie im Untermenü "Metadaten" die XML-Metadaten und das IdP-Zertifikat herunter, und notieren Sie sich die folgenden URLs, die später auf der ASA konfiguriert werden:
 - 1. SSO-URL
 - 2. Abmelde-URL
 - 3. Entitäts-ID
 - 4. Fehler-URL

Metadata		Recreate Certificate
Information for configuring a	pplications with Duo Access Gateway. Download XML metadata.	
Certificate	/C=US/ST=MI/L=Ann Arbor/O=Duo Security, Inc. Download certificate	
SHA-1 Fingerprint	2030-04-50 16.57.14	
SHA-256 Fingerprint		
SSO URL	https://explorer.cisco.com/dag/sam12/idp/SSOService.php	
Logout URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer	
Entity ID	https://explorer.cisco.com/dag/saml2/idp/metadata.php	
Error URL	https://explorer.cisco.com/dag/module.php/duosecurity/du	

-ASA-Konfiguration

Dieser Abschnitt enthält Informationen zur Konfiguration von ASA für die SAML-IDP-Authentifizierung und die grundlegende AnyConnect-Konfiguration. Das Dokument enthält die ASDM-Konfigurationsschritte und die CLI-Konfiguration, die für die Übersicht ausgeführt wird.

1. Duo Access Gateway-Zertifikat hochladen

A. Navigieren Sie zu "Konfiguration > Gerätemanagement > Zertifikatsverwaltung > Zertifizierungsstellenzertifikate", und klicken Sie auf "Hinzufügen".

B. Konfigurieren Sie auf der Seite "Install Certificate" (Zertifikat installieren) den Trustpoint-Namen: Duo_Access_Gateway.

C. Klicken Sie auf "Durchsuchen", um den Pfad für das DAG-Zertifikat auszuwählen, und klicken Sie nach der Auswahl auf "Zertifikat installieren".

Home Configuration Monitoring	Cisco ASDM 7.12(2) for ASA - 10.197.164.3	ob
Device Management	Save Vicence Dark Vicence Vicence Vicence Co	CI
 Device Management Management Access Licensing System Image/Configuration High Availability and Scalability Logging Smart Call-Home Cloud Web Security Security Cloud Web Security Cloud	 Configuration > Device Management > Certificate Management > CA Certificate Install Certificate Trustpoint Name: Duo_Access_Gateway Install from a file: //Users/pusaxena/Desktop/dag.crt Browse Paste certificate in PEM format: 	iils RL
	Use SCEP: Specify source Interface: None SCEP URL: http:// Retry Period: 1 Retry Count: 0 (Use 0 to indicate	unlimited retries)
Device Setup Firewall Remote Access VPN	M Help Cancel Install Certificate	ore Options
Device Management	Reset Apply	

2. Erstellen Sie einen lokalen IP-Pool für AnyConnect-Benutzer.

Navigieren Sie zu "Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools", und klicken Sie auf "Add".

			Cisco ASDM 7.12(2) for ASA - 10.197.164.3	
đ	Home	🍓 Configuration 🧕 Monitoring	🔜 Save 🔇 Refresh 🔇 Back 🕥 Forward 🦻 Help Type topic Go	cisco
🔳 Bookmarks 💼 Device List 💦		Monitoring Remote Access VPN Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localiza AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software Dynamic Access Policies Coup Policies Psec(IKEv2) Connection Profiles Psec(IKEv2) Connection Profiles Secure Mobility Solution Advanced Clientless SSL VPN Access AAA Server Groups Advanced Clientless SSL VPN Access AAA/Local Users Cartificate Management Language Localization Load Balancing DHCP Server DNS Device Setup Access VPN	Save Refresh R	itess itess
	8 8 [], [ite-to-Site VPN Device <u>M</u> anagement *	Reset Apply	

3. Konfigurieren der AAA-Servergruppe

A.: Konfigurieren Sie in diesem Abschnitt die AAA-Servergruppe, und geben Sie Details zum AAA-Server an, der die Autorisierung durchführt.

B. Navigieren Sie zu "Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups", und klicken Sie auf "Add" (Hinzufügen).

	Home 🖓 Configuration 🔯 Monitorin	g 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help Type topic Go	cisco				
L.	O O O Remote Access VPN	O O Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups					
e Lis	Introduction	AAA Server Groups					
evic	Network (Client) Access	Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts	Add				
	Clientless SSL VPN Access	Add AAA Server Group					
ookmarks	AAA Server Groups	AAA Server Group: ISE Protocol: RADIUS ᅌ	Edit Delete				
ă	Gamma Secure Desktop Manager Gamma Secure Desktop Manager Gamma Secure Desktop Manager	Accounting Mode: Simultaneous Single					
	B Language Localization	Paretivation Mode: O Depletion Timed					
	Sector Balancing	Reactivation mode. Oppletion Timed					
	P DHCP Server	Dead Time: 10 minutes					
	Advanced	Max Failed Attempts: 3					
		Enable interim accounting update					
		Opdate Interval: 24 Hours	Add				
		Enable Active Directory Agent mode	Edit				
		ISE Policy Enforcement	Delete				
		Enable dynamic authorization	Delete				
			Move Up				
		Dynamic Authorization Port: 1700	Move Down				
		Vise authorization only mode (no common password configuration required)	MOVE DOWN				
			Test				
		VPN3K Compatibility Option ¥					
	A Device Setup						
	Eirourall						
	riewaii						
	Remote Access VPN	Find:					
	Site-to-Site VPN						
	Device Management	LDAP Attribute Map	*				
	»	Reset Apply					

C. Klicken Sie auf derselben Seite im Abschnitt "Server in der ausgewählten Gruppe" auf "Hinzufügen", und geben Sie die IP-Adresse des AAA-Servers an.

Home 🍕 Configuration 🛐 Monitoring [🚽 Save 🔇 Refresh	🕒 Back 🔘	Forward 💡 Help	Type topic Go			cis
O O O Remote Access VPN	○ ○ O <u>Configur</u>	ation > Remot	e Access VPN > A	AA/Local Users	> <u>AAA Ser</u>	ver Groups	
? Introduction	AAA Server Grou	ips					
Network (Client) Access	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add
AnyConnect Connection Profiles	ISE	RADIUS	Single	Depletion	10	3	
AnyConnect Client Profile	LOCAL	LOCAL					Edit
T AnyConnect Client Software							Delete
Poince and the second s							
Group Policies			Add AAA Serve	r			
IPsec(IKEv1) Connection Profiles IPsec(IKEv2) Connection Profiles	Server Group	(SF				
Secure Mobility Solution	Interface Nam						
Address Assignment	interface Nam	ie.	outside			_	
Assignment Policy	Server Name	or IP Address:	10.106.44.77				
Address Pools	Timeout:		10 seconds				
Glientless SSL VPN Access							
AAA/Local Users	RADIUS Paran	neters				(Add
AAA Server Groups	Server Auth	entication Port	: 1645				5 .4%
LDAP Attribute Map	Server Acco	ounting Port:	1646				Edit
Local Users	Detroclator		10 seconds				Delete
Secure Desktop Manager Secure Desktop Manager	Ketry Interv	ar:	10 seconds				
Anguage Localization	Server Secr	et Key:					Move Up
😤 Load Balancing	Common P	assword:					Move Down
P DHCP Server	ACL Netma	sk Convert:	Standard				Test
JNS DNS	Microsoft (HAD/2 Canable					Test
	MICrosoft C	Indevz Capabi	e. 💟				
💑 <u>D</u> evice Setup	SDI Messages						
👬 Firewall	Message 1	Table				*	
Remote Access VPN		Help	Cancel	ОК			
Site-to-Site VPN		Max			_		
Device Management	LDAP Attribute	мар					
			Res	et Apply			

4. AnyConnect-Clientsoftware zuordnen

A. Map the AnyConnect client software webdeploy image 4.8.03052 for windows to be used for WebVPN

B. Navigieren Sie zu "Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client) > AnyConnect-Clientsoftware", und klicken Sie auf "Hinzufügen".



5. Konfigurieren Sie die als Ergebnis der ISE weitergeleitete ACL.

A. Navigieren Sie zu "Configuration > Firewall > Advanced > ACL Manager", und klicken Sie auf Add, um die Umleitungszugriffskontrollliste hinzuzufügen. Die Einträge sehen nach der Konfiguration wie folgt aus:

					Cisco ASDM 7.12(2	2) for ASA - 10	.197.164.3			
	Home	onfiguration 🛐 Monito	ring 🔓	🛛 Save 💽 F	Refresh 🔇 Back	Forward 🖸	? Help Type topic G	0		cisco
	00	O Firewall		O Configu	ration > Firewall >	Advanced >	ACL Manager			
e Lis		Access Rules	4	🗣 Add 🗸 🍯 Edit 🍵 Delete 🗇 🖌 👗 🐂 🌉 🗸 🔍 S. Find 🔜 Export 🝷						
Devic		NAT Rules	#	Enabled	Source	Se	Destination	Security Group	Destination Service	Action
	4		🔻 re	direct						
		Filter Rules	1	Image: A start and a start	🧼 any		🧼 any		🚥 domain	🕴 Deny
rks		Ethertype Rules	2	Image: A start of the start	🧼 any		🖳 10.197.243.116			🕴 Deny
kma	6	Public Servers	3	Image: A start of the start	🧼 any		🧼 any		🥵 icmp	🕴 Deny
Boo	UR	URL Filtering Servers	4	Image: A start of the start	🧼 any		🏈 any		≖> ip	🖌 Permit
	Z	Threat Detection	5	Image: A start of the start	🧼 any		🧇 any		🐵 http	🖌 Permit
	0	Identity Options	_							
	2	Identity by TrustSec								
		VM Attribute Agent								
		Botnet Traffic Filter								
		Unified Communications								
		Advanced								
		Anti-Spoofing								
	▶	🖻 Certificate Management								
		😻 Fragment								
	▶	No. IP Audit								
		SUNRPC Server								
		TCP Options								
		S Global Timeouts								
		Standard ACL								
		Per-Session NAT Rules								
		<u>D</u> evice Setup								
	8.	F <u>i</u> rewall								
	3	Remote Access VPN								
		Site-to-Site VPN		ollapse All	Expand All					
		Device <u>M</u> anagement			Expanse All					
		»					Reset Apply)		

6. Bestehende Gruppenrichtlinie validieren

A. Bei dieser Konfiguration wird die standardmäßige Gruppenrichtlinie verwendet. Diese kann angezeigt werden unter: "Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client) > Gruppenrichtlinien"



- 7. Verbindungsprofil konfigurieren
- A. Erstellen Sie ein neues Verbindungsprofil, mit dem AnyConnect-Benutzer eine Verbindung

herstellen.

B. Navigieren Sie zu "Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client) > AnyConnect-Verbindungsprofile", und klicken Sie auf "Hinzufügen".

		Cisco ASDM 7.1	12(2) for ASA - 10.	197.164.3		
👌 Home 🦓 Configuration 📴 Monitori	ng 🔚 Save 🔇	Refresh 🔇 Bao	ck 🔘 Forward	? Help Type topic	Go	CISC
O Remote Access VPN	 ○ ○ ○ ○ <u>Config</u>	ration > Remot	e Access VPN > N	letwork (Client) Ac	cess > AnyConnect Conne	ction Profiles
 Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Local 	The security a initial client o tunnel as well	appliance automa leployment requi as SSL tunnel wi	tically deploys the res end-user admi ith Datagram Tran	e Cisco AnyConnect nistrative rights. Th sport Layer Security	VPN Client to remote users ne Cisco AnyConnect VPN Cli (DTLS) tunneling options.	upon connection. The ent supports IPsec (IK
AnyConnect Client Profile		co AnyConnect	VPN Client access	on the interfaces s	lastad in the table below	
Dynamic Access Policies	Enable Cl	sco AnyConnect	VPN Client access	on the interfaces se	elected in the table below	1
Group Policies	SSL access m	ust be enabled if	you allow AnyCon	nect client to be lat	inched from a browser (Web	Launch) .
IPsec(IKEv1) Connection Profiles	Interface	Allow Access	Enable DTLS	Allow Access	s Enable Client Services	During Cardification
IPsec(IKEv2) Connection Profiles	outside					Device Certificate
 Secure Mobility Solution Address Assignment 						Port Settings
Load Balancing PLCP Server DHCP Server Advanced	 Allow use Shutdowr Connection Prof Connection p from certifica 	r to select conne portal login pag files rofile (tunnel gro te to connection	ection profile on the le. up) specifies how profile <u>here</u> .	user is authenticate	ed and other parameters. You	i can configure the ma
	Add A	Edit Delete	Find:		Match Case	
	Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
A Device Setup	DefaultRAGr				AAA(LOCAL)	DfltGrpPolicy
Sirewall	DefaultWEBV			CANIL LINE	AAA(LOCAL)	DfltGrpPolicy
Remote Access VPN	TG_SAML			SAML_User	s Sami	DfltGrpPolicy
Site-to-Site VPN	Let group connectio	URL take preced on profile that ma	ence if group URL atches the certifica	and certificate map te map will be used	match different connection	profiles. Otherwise, th
Device <u>M</u> anagement				Reset App	ly	

C. Konfigurieren Sie die folgenden Details für das Verbindungsprofil:

Name	TG_SAML
Aliase	SAML_Benutzer
Methode	SAML
AAA-Servergruppe	Lokal
Client-Adresspools	AC-Pool
Gruppenrichtlinie	DfltGrpPolicy

Basic Advanced	Name:	G_SAML)
Advanced	Aliases:	AML_Users)
	Authentication		-
	Method:	SAML	
	AAA Server Group:	LOCAL	Manage
		Use LOCAL if Server Group fails	
	SAMI Identity Provider		
	SAML Server :	https://explorer.cisco.com/dag/saml2/idp/metadata.php	Manage
	DHCP Servers		
		None DHCP Link DHCP Subnet	
	Client Address Pools:	C Pool	Select
	Client ID C Address Pools.	<u></u>	Colort
	Client IPv6 Address Pools:		Select
	Default Group Policy		_
	Group Policy:	fltGrpPolicy	Manage
	(Following fields are linked to	attribute of the group policy selected above.)	
	Enable SSL VPN client p	protocol	
	Enable IPsec(IKEv2) clie	nt protocol	
	DNS Servers:		
	WINS Servers:		
	Domain Name:		
Eindi		A Novt A Draviour	
rinu.		Wext Previous	
	He	lp Cancel OK	

D. Konfigurieren Sie auf derselben Seite die Details des SAML Identity Providers, die wie folgt aussehen:

ID der IDP- Einheit	https://explorer.cisco.com/dag/saml2/idp/metadata.php
Anmelde- URL	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
Abmelde- URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SingleService.php
Basis- URL	https://firebird.cisco.com

E. Klicken Sie auf "Verwalten > Hinzufügen"

	Add SSO Server
IDP Entity ID:	https://explorer.cisco.com/dag/saml2/idp/metadata.php
Settings	
Sign In URL:	https ᅌ :// explorer.cisco.com/dag/saml2/idp/SSOService.php
Sign Out URL:	https ᅌ :// explorer.cisco.com/dag/saml2/idp/SingleLogoutSe
Base URL	https ᅌ :// firebird.cisco.com
Identity Provider Certificate	Duo_Access_Gateway:o=Duo Security Inc., I=Ann Ar
Service Provider Certificate:	ID_CERT:cn=firebird.cisco.com:cn=SHERLOCK-CA, dc=c
Request Signature:	None 📀
Request Timeout:	1200 seconds (1-7200)
Enable IdP only accessible on Internal Network	
Request IdP re-authentication at login	
Help	Cancel

F. Definieren Sie im Abschnitt "Erweitert" für das Verbindungsprofil den AAA-Server für die Autorisierung.

Navigieren Sie zu "Erweitert > Autorisierung", und klicken Sie auf "Hinzufügen".

		Edit AnyConnect Connection Profile: TG_SAML
Γ	Basic	Authorization Server Group
	Advanced	Server Group: ISE
	General	
	Client Addressing	Users must exist in the authorization database to connect
	Authentication	
	Secondary Authentic	Interface-specific Authorization Server Groups
	Authorization	💠 Add) 🗹 Edit 📋 Delete
	Accounting	Assign Authorization Service Crown to Interface
	Group Alias/Group L	 Assign Authorization Server Group to Interface
		Interface: Outside
		Server Group: ISE 📦 Manage
		Help Cancel OK

G. Definieren Sie unter Gruppenalias den Verbindungsalias.

Navigieren Sie zu "Erweitert > Gruppenalias/Gruppen-URL", und klicken Sie auf "Hinzufügen".

	Edit AnyConnect Connection Profile: TG_S	SAML
Basic Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting Group LIBL	 Enable the display of Radius Reject-Message on Enable the display of Securid messages on the list Connection Aliases This SSL VPN access method will present a list of alia the Login Page Setting in the main panel to complete Add Connection Aliase 	a the login screen when authentication is rejected ogin screen iases configured for all connection profiles. You mus te the configuration.
	Alias: SAML_Users	■ the connection profile, without the need for user s

H. Damit ist die ASA-Konfiguration abgeschlossen. Dies sieht wie unten auf der Befehlszeilenschnittstelle (CLI) aus.

```
I
hostname firebird
domain-name cisco.com
I
I
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
Т
   -----Client pool configuration------Client pool configuration------
1 - -
1
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
Т
   ------Redirect Access-list-----
1 -
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
    -----AAA server configuration------AAA server
1
T
aaa-server ISE protocol radius
authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
key *****
!
!-----Configure Trustpoint for Duo Access Gateway Certificate-----
1
crypto ca trustpoint Duo_Access_Gateway
enrollment terminal
crl configure
ï
   -----Configure Trustpoint for ASA Identity Certificate------
!--
I
crypto ca trustpoint ID_CERT
enrollment terminal
 fqdn firebird.cisco.com
```

```
subject-name CN=firebird.cisco.com
 ip-address 10.197.164.3
 keypair ID_RSA_KEYS
no ca-check
crl configure
ļ
   ----Enable AnyConnect and configuring SAML authentication-----
! -
I
webvpn
 enable outside
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
 anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
 anyconnect enable
 saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
 url sign-in https://explorer.cisco.com/dag/saml2/idp/SSOService.php
 url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
 base-url https://firebird.cisco.com
 trustpoint idp Duo_Access_Gateway
 trustpoint sp ID_CERT
 no signature
 no force re-authentication
 timeout assertion 1200
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
I
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
ï
! -
   -----Tunnel-Group (Connection Profile) Configuraiton-------
I
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
 address-pool AC_Pool
authorization-server-group ISE
 accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
 authentication saml
group-alias SAML_Users enable
saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
I
```

-ISE-Konfiguration

1. Cisco ASA als Netzwerkgerät hinzufügen

Klicken Sie unter "Administration > Network Resources > Network Devices" auf "Add" (Hinzufügen).

Konfigurieren Sie den Namen des Netzwerkgeräts, die zugehörige IP-Adresse, und konfigurieren Sie unter "Radius Authentication Settings" den "Shared Secret", und klicken Sie auf "Save"

(Speichern).

Network Devices List > ASA
Network Devices
* Name ASA
IP Address * IP : 10.197.164.3 / 32
* Device Profile device Cisco 💌 🕀
Model Name
Software Version
* Network Device Group
Location All Locations 📀 Set To Default
IPSEC No Set To Default
Device Type All Device Types 📀 Set To Default

 RADIUS Authentication Settings 	
RADIUS UDP Settings	
Protocol	RADIUS
* Shared Secret	••••• Show
Use Second Shared Secret	
	Show
CoA Port	1700 Set To Default
RADIUS DTLS Settings	
DTI S Paquired	
Shared Secret	radius/dtls
CoA Port	2002 Set To Default
	2003 Set to Detault
Issuer CA of ISE Certificates for CoA	Select if required (optional)
DNS Name	
Canaral Sattinga	
General Settings	
Enable KeyWrap	
* Key Encryption Key	Show
* Message Authenticator Code Key	Show
Key Input Format	ASCII HEXADECIMAL
TACACS Authentication Settings	
▶ SNMP Settings	
Advanced TrustSec Settings	
Parat	
INCSCL .	

2. Installation der neuesten Statusaktualisierungen

Navigieren Sie zu "Administration > System > Settings > Posture > Updates", und klicken Sie auf "Update Now" (Jetzt aktualisieren).

Posture Updates	
• Web	Offline
* Update Feed URL	https://www.cisco.com/web/secure/spa/posture-update.xml Set to Default
Proxy Address	72.163.217.104
Proxy Port	80 HH MM SS
Automatically che	ck for updates starting from initial delay 06 - 00 - 18 - every 2 hours
Save	date Now Reset

Last successful update on	2020/05/07 15:15:05
Last update status since ISE was started	No update since ISE was started. (
Cisco conditions version	224069.0.0.0
Cisco AV/AS support chart version for windows	171.0.0.0
Cisco AV/AS support chart version for Mac OSX	91.0.0.0
Cisco supported OS version	41.0.0.0

Update Information

3. Laden Sie das Compliance-Modul und das AnyConnect Headend-Bereitstellungspaket auf die ISE hoch.

Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Client-Bereitstellung > Ressourcen". Klicken Sie auf "Hinzufügen", und wählen Sie je nachdem, ob die Dateien von der lokalen Workstation oder von der Cisco Website abgerufen werden sollen, "Agenten-Ressourcen von der lokalen Festplatte" oder "Agenten-Ressourcen von der Cisco Website" aus.

In diesem Fall wählen Sie zum Hochladen von Dateien von der lokalen Workstation unter Kategorie "Von Cisco bereitgestellte Pakete" aus, klicken auf "Durchsuchen", wählen die erforderlichen Pakete aus und klicken auf "Senden".

In diesem Dokument wird "anyconnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg" als Compliance-Modul und "anyconnect-win-4.8.03052-webdeploy-k9.pkg" als AnyConnect Headend-Bereitstellungspaket verwendet.

Agent Resources From Local Disk > Agent Resources From Local Disk

Agent	Resources	From	Local	Disk
-------	-----------	------	-------	------

Category	Cisco Provided Packages Browse anyconnect-win-4.8.03	052-webdeploy-k9.pkg		
	AnyConnect Uploaded Resource	S		
	Name	Туре	Version	Description
	AnyConnectDesktopWindows 4.8.30	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie

Submit Cancel

4. AnyConnect-Posture-Profil erstellen

A. Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Client-Bereitstellung > Ressourcen". Klicken Sie auf "Hinzufügen", und wählen Sie "AnyConnect Posture Profile" aus.

B. Geben Sie den Namen für AnyConnect Posture Profile ein, und konfigurieren Sie den Servernamen als "*" unter "Servernamen", und klicken Sie auf "Speichern".

ISE Posture Agent Profile Settings > Anyconnect Posture Profile

* Name:	Anyconnect Posture Profile	
Description		
		11.

Posture Protocol

Parameter	Value	Notes	Description		
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure		
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.		
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.		
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to		
Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. ", cisco.com"		
Call Home List		List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN.Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.		
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached		

5. AnyConnect-Konfiguration erstellen

A. Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Client-Bereitstellung > Ressourcen". Klicken Sie auf "Hinzufügen", und wählen Sie "AnyConnect-Konfiguration" aus.

B. Wählen Sie AnyConnect-Paket, geben Sie den Konfigurationsnamen ein, und wählen Sie das erforderliche Compliance-Modul aus.

C. Aktivieren Sie unter "AnyConnect Module Selection" das Kontrollkästchen "Diagnostic and Reporting Tool".

D. Wählen Sie unter "Profile Selection" (Profilauswahl) die Option Posture Profile und klicken Sie auf "Save" (Speichern).

AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package	AnyConnectDesktopWindows 4.8.3052.0	
* Configuration Name	AnyConnect Configuration	
Description:		
DescriptionV	Value Notes	
* Compliance Module	AnyConnectComplianceModuleWindows 4.3.1250.614	
AnyConnect Module Selection		
ISE Posture		
VPN		
Network Access Manager		
Web Security		
AMP Enabler		
ASA Posturo		

ASA Posture Network Visibility Umbrella Roaming Security Start Before Logon Diagnostic and Reporting Tool

Profile Selection

		_
* ISE Posture	Anyconnect Posture Profile	J
VPN		,
Network Access Manager		,
Web Security		,
AMP Enabler		-
Network Visibility		,
Umbrella Roaming Security		,
Customer Feedback		,

6. Client-Bereitstellungsrichtlinie erstellen

A. Navigieren Sie zu "Richtlinie > Client-Bereitstellung"

B. Klicken Sie auf "Bearbeiten" und wählen Sie "Regel oben einfügen".

C. Geben Sie den Regelnamen ein, wählen Sie das erforderliche Betriebssystem aus, und wählen Sie unter Results (unter "Agent" > "Agentenkonfiguration") die in Schritt 5 erstellte AnyConnect-Konfiguration aus, und klicken Sie auf "Speichern".

cisco Ide	ntity Services Eng	gine	Home	•	Context Visibility	y I	Operations	▼ Policy		Administration	Work Centers			License Warning 🔺	্ 💡	o 0
Policy Set	s Profiling Post	ure	Client Provi	sionin	g + Policy Ele	ements										
Client Pro Define the C For Agent C For Native S	visioning Policy lient Provisioning Pol onfiguration: version of upplicant Configuration	licy to d of agen on: wizi	determine wi nt, agent pro ard profile a	hat us file, ag	ers will receive ugent compliance wizard. Drag and	pon log module I drop r	gin and user sess b, and/or agent or ules to change th	ion initiation ustomization ne order.	n: n packi	age.						
*																
	Rule Name			k	fentity Groups		Operating Syst	ems		Other Condition	is .		Results			
	IOS			lf A	liny	and	Apple iOS All		and	Condition(s)		then	Cisco-ISE-NSP			Edit 🕶
Image:	Android			lf A	liny	and	Android		and	Condition(s)		then	Cisco-ISE-NSP			Edit 🔻
1	Windows_10			lf A	liny	and	Windows 10 (/	All)	and	Condition(s)		then	AnyConnect Configuration			Edit 👻
	Windows			if A	iny	and	Windows All		and	Condition(s)		then	CiscoTemporalAgentWi ndows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP			Edit 🔻
	MAC OS			H A	lny	and	Mac OSX		and	Condition(s)		then	CiscoTemporalAgentOS X 4.7.00135 And Mac03xSPWizard 2.1.0.42 And Cisco-ISE- NSP			Edit 🔻
	Chromebook			If A	liny	and	Chrome OS A		and	Condition(s)		then	Cisco-ISE-Chrome-NSP			Edit 🕶
Save	Reset															

7. Eine Statusbedingung erstellen

A. Navigieren Sie zu "Richtlinie > Richtlinienelemente > Bedingungen > Status > Dateibedingung".

B. Klicken Sie auf "Hinzufügen", und konfigurieren Sie den Bedingungsnamen "VPN_Posture_File_Check", das erforderliche Betriebssystem als "Windows 10(All)", den Dateityp als "FileExistence", den Dateipfad als "ABSOLUTE_PATH" und den vollständigen Pfad und Dateinamen als "C:\custom.txt". Wählen Sie Dateioperator als "Exists" aus.

C. In diesem Beispiel wird das Vorhandensein einer Datei mit dem Namen "custom.txt" unter Laufwerk C: als Dateibedingung verwendet.

cisco Identity Services Engine	Home	► Operations ▼ Policy	► Administration	➤ Work Centers
Policy Sets Profiling Posture Cl	lient Provisioning Policy Element	nts		
Dictionaries - Conditions + Result	S			
Library Conditions Smart Conditions Time and Date Profiling	File Conditions List > VPN_Post File Condition * Name	ure_File_Check		
▼ Posture	* Operating System	ndows 10 (All) 🔶		
Anti-Malware Condition Anti-Spyware Condition	Compliance Module Any * File Type File	Existence		
Anti-Virus Condition Application Condition	* File Operator	sts v	C:\custom.txt	0
Disk Encryption Condition	Save			

8. Aktion zur Statusbehebung erstellen

Navigieren Sie zu "Policy > Policy Elements > Results > Posture > Remediation Actions" (Richtlinie > Richtlinienelemente > Ergebnisse > Status > Korrekturmaßnahmen), um eine entsprechende Dateibereinigungsaktion zu erstellen. Dieses Dokument verwendet "Nur Nachrichtentext" als Korrekturmaßnahmen, die im nächsten Schritt konfiguriert werden.

9. Statusanforderungsregel erstellen

A. Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Status > Anforderungen".

B. Klicken Sie auf "Bearbeiten" und wählen Sie dann "Neue Anforderung einfügen".

C. Konfigurieren Sie den Bedingungsnamen "VPN_Posture_Requirement", das erforderliche Betriebssystem als "Windows 10(Alle)", das Compliance-Modul als "4.x oder höher", den Statustyp als "AnyConnect".

D. Bedingungen wie "VPN_Posture_File_Check" (erstellt in Schritt 7) und unter "Korrekturmaßnahmen" Aktion als "Nur Nachrichtentext" auswählen und die benutzerdefinierte Nachricht für Agent-Benutzer eingeben

						-	
0	Benulsemente					(*	
thentication	Requirements	Denseties Original	Occurring the state	Destars Trace	One dillere	Demodeline Asless	
hadration	quirement_win	Operating System	Compliance Module	Posture Type	eck	Remediations Actions	
nonzation	Default_Hardware_Attributes_Re quirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Ch eck	then Select Remediations	Ec
filing	Default_Firewall_Requirement_W in	for Windows All	using 4.x or later	using AnyConnect	met if Default_Firewall_Conditi on_Win	then Default_Firewall_Remedi ation_Win	Ed
ure	Default_Firewall_Requirement_M ac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_Firewall_Conditi on_Mac	then Default_Firewall_Remedi ation_Mac	Ed
mediation Actions	USB_Block_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only	Er
uirements	Any_AM_Installation_Win_tempo ral	for Windows All	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only	Ed
t Provisioning	Any_AM_Installation_Mac_tempo ral	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only	Ec
	Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition n_Win	then Select Remediations	Ec
	Default_AppVis_Requirement_M ac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations	Ed
	Default_Hardware_Attributes_Re quirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Ch eck	then Select Remediations	Ed
	Default_Hardware_Attributes_Re quirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Ch eck	then Select Remediations	Ed
	Default_Firewall_Requirement_W in_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Conditi on_Win	then Default_Firewall_Remedi ation_Win	Ed
	Default_Firewall_Requirement_M ac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Conditi on_Mac	then Default_Firewall_Remedi ation_Mac	Ed
	VPN_Posture_Requirement	for Windows 10 (All)	using 4.x or later	using AnyConnect	met if VPN_Posture_File_Chee	then Message Text Only	E

- 10. Erstellen einer Statusrichtlinie
- A. Navigieren Sie zu "Policys > Status"

B. Konfigurieren Sie den Regelnamen als "VPN_Posture_Policy_Win", das erforderliche
Betriebssystem als "Windows 10(Alle)", das Kompatibilitätsmodul als "4.x oder höher", den
Statustyp als "AnyConnect" und die Anforderungen als "VPN_Posture_Requirement", wie in Schritt
9 konfiguriert

Identity	Services Engine	B Home I Context Visib	ility > Operations		ation				License Warning 🔺 🔍	0 0
iets I	Profiling Posture	Client Provisioning Policy	Elements							
Belle										
Postur	Y Policy by configu	ring rules based on operating system	m and/or other conditio	05.					*	
Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions		Requirements	
2	Policy Options	Default_AppVis_Policy_Win	f Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Default_AppVis_Requir ement_Win	
)	Policy Options	Default_AppVis_Policy_Win_te In mporal	f Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	Default_AppVis_Requir ement_Win_temporal	
)	Policy Options	Default_Firewall_Policy_Mac	f Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then	Default_Firewall_Requir ement_Mac	
)	Policy Options	Default_Firewall_Policy_Mac_t in emporal	f Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then	Default_Firewall_Requir ement_Mac_temporal	
	Policy Options	Default_Firewall_Policy_Win	f Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Default_Firewall_Requir ement_Win	
)	Policy Options	Default_Firewall_Policy_Win_te mporal	Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	Default_Firewall_Requir ement_Win_temporal	
)	Policy Options	Default_Hardware_Attributes_P II olicy_Mac	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then	Default_Hardware_Attri butes_Requirement_Ma c	
)	Policy Options	Default_Hardware_Attributes_P II olicy_Mac_temporal	Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then	Default_Hardware_Attri butes_Requirement_Ma c_temporal	
,	Policy Options	Default_Hardware_Attributes_P I olicy_Win	f Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Default_Hardware_Attri butes_Requirement_Wi n	
)	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	Default_Hardware_Attri butes_Requirement_Wi n_temporal	
)	Policy Options	Default_USB_Block_Policy_Winn	f Any	and Windows All	and 4.x or later	and AnyConnect	and	then	USB_Block	
	Policy Options	Default_USB_Block_Policy_Win_temporal	Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	USB_Block_temporal	
	Policy Options	VPN_Posture_Policy_Win	f Any	and Windows 10 (All)	and 4.x or later	and AnyConnect	and	then	VPN_Posture_Require	

11. Erstellen dynamischer Zugriffskontrolllisten (DACLs)

Navigieren Sie zu "Policy > Policy Elements > Results > Authorization > Downlodable ACLS" (Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > herunterladbare ACLS), und erstellen Sie die DACLs für verschiedene Statusstatus.

In diesem Dokument werden die folgenden DACLs verwendet.

A. Status unbekannt: Ermöglicht Datenverkehr zu DNS-, PSN- und HTTP- sowie HTTPS-Datenverkehr

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	lient Provisioning Policy Elements
Dictionaries Conditions Result	IS
Authentication Authorization	Downloadable ACL List > PostureUnknown Downloadable ACL * Name PostureUnknown
Authorization Profiles	Description
Downloadable ACLs	IP version • IPv4 IPv6 Agnostic
▶ Profiling	* DACL Content 1234567 permit udp any any eq domain
▶ Posture	2131415 permit top any any eq 443
Client Provisioning	9202122 2324252 6272829 3031323 3343536
	Check DACL Syntax
	Save

B. Status nicht konform: Verweigert den Zugriff auf private Subnetze und lässt nur Internetdatenverkehr zu

the light of the	
Policy Sets Profiling Posture Client Provisioning Policy Elements	
Dictionaries Conditions	
Authentication Downloadable ACL List > PostureNonCompliant Downloadable ACL Downloadable ACL * Authorization * Name PostureNonCompliant	
Authorization Profiles Description	
Downloadable ACLs	
Profiling * DACL Content 1234567 deny ip any 10.0.0.255.0.0.0	
8910111 deny ip any 172.16.0.0 255.240.0.0 Posture 2131415 deny ip any 192.168.0.0 255.255.0.0 1647181 permit ip any any	
> Client Provisioning 9202122 2324252 6272829 3031323 3343536 > Check DACL Syntax 0	
Save	

C. Posture Compliant: Ermöglicht den gesamten Datenverkehr für Endbenutzer, die Posture Compliant sind

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	lient Provisioning Policy Elements
Dictionaries	ts
Authentication Authorization	Downloadable ACL List > PostureCompliant Downloadable ACL * Name PostureCompliant
Authorization Profiles	Description
Downloadable ACLs	IP version OIPv4 OPv6 Agnostic ()
▶ Profiling	* DACL Content 1234567 permit ip any any
▶ Posture	8910111 2131415 1617181
Client Provisioning	9202122 2324252 6272829 3031323 3343536
	Check DACL Syntax
	Save

12. Autorisierungsprofile erstellen

Navigieren Sie zu "Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile".

A. Autorisierungsprofil für unbekannten Status

Wählen Sie DACL "PostureUnknown" (Status unbekannt), aktivieren Sie die Option Web Redirection (Webumleitung), wählen Sie Client Provisioning (Status) aus, konfigurieren Sie den Namen der Umleitungs-ACL "redirect" (Umleitung) (auf dem ASA zu konfigurieren), und wählen Sie das Client Provisioning Portal (Standard) aus.

ullully worth Oracless Factor			0.0		
cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning	~ •	•	
Policy Sets Profiling Posture Cl	ent Provisioning Policy Elements				
Dictionaries + Conditions - Result	3				
0					
• Authentication	Authorization Profiles > Posture Redirect				
Addientication	Authorization Profile				
- Authorization	* Name Posture Redirect				
Authorization Profiles	Description				
Downloadable ACLs	* Access Type Access ACCEPT T				
Profiling	Network Device Profile 🗮 Cisco 💌 🕀				
Posture	Service Template				
Client Provisioning	Track Movement 🗌 🕖				
-	Passive Identity Tracking 🗌 🕧				
	DACL Name PostureUnknown				

 Glient Provisioning 	Web Redirection (CWA, MDM, NSP, CPP) Client Provisioning (Posture) ACL (redirect Client Provisioning Portal (default)
	▼ Advanced Attributes Settings
	Select an Rem
	▼ Attributes Details
	Access Type = ACCESS_ACCEPT DACL = PostureUnknown dscs-ar-pair = url-redirect-ad-irredirect dscs-ar-pair = url-redirect-ad-irredirect dscs-ar-pair = url-redirect=https://ip.port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp
	Save Reset

B. Autorisierungsprofil für nicht konforme Haltung

Wählen Sie DACL "PostureNonCompliant" aus, um den Zugriff auf das Netzwerk einzuschränken.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers License Warning
Policy Sets Profiling Posture C	Illent Provisioning Policy Elements
Dictionaries Conditions Resul	<u>16</u>
0	Autoristics Devices Nan Camellast
Authentication	Authorization Profile
- Authorization	* Name Posture Non Compliant
Authorization Profiles	Description
Downloadable ACLs	* Access Type (IACCESS ACCEPT *)
Profiling	Network Device Profile 🗮 Cisco 🔻 🕀
▶ Posture	Service Template
Client Provisioning	Track Movement 🔐
	Pasalve Identity Tracking 🔄 🕧
	✓ Common Tasks
	DACL Name PostureNonCompliant
	▼ Attributes Details
	Access Type = ACCESS_ACCEPT DACL = PostureNonCompliant
	Sive Rest.

C. Autorisierungsprofil für Posture Compliant

Wählen Sie DACL "PostureCompliant" aus, um vollständigen Zugriff auf das Netzwerk zu ermöglichen.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	् 🔞	o 0
Policy Sets Profiling Posture C	Zient Provisioning Policy Elements			
Dictionaries Conditions Resu	hs			
0				
Authentication	Authorization Profile			
- Authorization	* Name Full Access			
Authorization Profiles	Description			
Downloadable ACLs	* Access Type Access ACCEPT Y			
Profiling	Network Device Profile 📾 Claco 💌 🕀			
Posture	Service Template			
Client Provisioning	Track Movement 🔄 🕧			
	Passive identity Tracking 0			
	Common Tasks DACL Name PostureCompliant			
	▼ Attributes Details			
	Access Type = ACCESS_ACCEPT DACL = PERMIT_ALL_IFV4_TRAFFIC		11.	
	Sive Reset			

12. Autorisierungsrichtlinien konfigurieren

Verwenden Sie die im vorherigen Schritt konfigurierten Autorisierungsprofile, um drei Autorisierungsrichtlinien für "Posture Compliant", "Posture Non-Compliant" und "Posture Unknown" zu konfigurieren.

Die allgemeine Bedingung "Session: Posture Status" wird verwendet, um die Ergebnisse der einzelnen Richtlinien zu bestimmen.

dialla Idei	ntity Service	es Engine Home → Conte	ext Visibility	y > Operations	Policy Administration	 Work Centers 					License Warning	<u> </u>	• • •
Policy Set	s Profiling	Posture Client Provisioning	 Policy E 	lements									
Policy S	<mark>ets →</mark> De	fault									Reset Policyset Hitcoun	s Res	save
	Status	Policy Set Name	Descrip	ption	Conditions						Allowed Protocols / Serv	er Sequence	Hits
Search													
	0	Default	Default	policy set							Default Network Access	x • +	49
> Authe	ntication Po	blicy (3)											
> Autho	rization Poli	icy - Local Exceptions											
> Autho	rization Poli	icy - Global Exceptions											
✓ Autho	rization Poli	icy (15)											
							ł	Results					
+	Status	Rule Name	Cond	litions			1	Profiles		Security Groups	S	Hits	Actions
Search													
	Ø	Anyconnect Posture Compliant	ĥ	Session PostureStatu	s EQUALS Compliant		[(×Full Access)	+	Select from list	- +	6	٩
	ø	Anyconnect Posture Non Compliant	ĥ	Session PostureStatu	s EQUALS NonCompliant			× Posture Non Compliant	+	Select from list	- +	0	٥
	Ø	Anvronnert Posture Unknown		P Network Acc	cess-Device IP Address EQUALS 1	0.197.164.3		× Posture Redirect	+	Select from list	· +	13	ò
	Ľ	Paryconnect Osture Onkilowi	AND	E Session-Pos	stureStatus EQUALS Unknown							.5	~

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Führen Sie den folgenden Befehl auf der ASA aus, um zu überprüfen, ob der Benutzer erfolgreich authentifiziert wurde.

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username : _585b5291f01484dfd16f394be7031d456d314e3e62 Index : 125 : 10.197.243.143 Assigned IP : explorer.cisco.com Public IP Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel : AnyConnect Premium License Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Bytes Tx : 16404 Bytes Rx : 381 : 16 Pkts Rx Pkts Tx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : TG_SAML Login Time : 07:05:45 UTC Sun Jun 14 2020 Duration : 0h:00m:16s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5a4030007d0005ee5cc49 Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 125.1 Public IP : 10.197.243.143 Encryption : none Hashing : none TCP Src Port : 57244 TCP Dst Port : 443 Auth Mode : SAML Idle TO Left : 29 Minutes Idle Time Out: 30 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 7973 Bytes Rx : 0 Pkts Tx : 6 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: : 125.2 Tunnel ID Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 57248 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 7973 Bytes Rx : 0 Pkts Tx Pkts Rx : 0 : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PostureUnknown-5ee45b05 DTLS-Tunnel: Tunnel ID : 125.3 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 : SHA384 Hashing Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 49175 UDP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 458 Bytes Rx : 381 Pkts Tx : 4 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name :

#ACSACL#-IP-PostureUnknown-5ee45b05

ISE Posture: Redirect URL : https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&po Redirect ACL : redirect

Nach Abschluss der Statusüberprüfung wird der Benutzerzugriff auf den vollständigen Zugriff geändert, wie in der DACL im Feld "Filter Name" (Filtername) gezeigt.

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username	: _585b5291f01484dfd16f394be7031d456d314e3e62
Index	: 125
Assigned IP	: explorer.cisco.com Public IP : 10.197.243.143
Protocol	: AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License	: AnyConnect Premium
Encryption	: AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing	: AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx	: 16404 Bytes Rx : 381

Pkts Tx : 16 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : TG_SAML Login Time : 07:05:45 UTC Sun Jun 14 2020 : 0h:00m:36s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5a4030007d0005ee5cc49 Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 125.1 : 10.197.243.143 Public IP Encryption : none : none Hashing TCP Src Port : 57244 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Client Ver Bytes Tx : 7973 Bytes Rx : 0 Pkts Tx : 6 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 125.2 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 57248 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes : Windows Client OS Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 : 7973 Bytes Tx Bytes Rx : 0 Pkts Tx : 6 Pkts Rx : 0 Pkts Rx Drop : 0 Pkts Tx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3 DTLS-Tunnel: Tunnel ID : 125.3 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 49175 UDP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes : Windows Client OS Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 : 458 Bytes Tx Bytes Rx : 381 Pkts Tx Pkts Rx : 4 : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name :

Um zu überprüfen, ob die Autorisierung auf der ISE erfolgreich durchgeführt wurde, navigieren Sie zu "Operations > RADIUS > Live Logs" (Vorgänge > RADIUS > Live-Protokolle).

In diesem Abschnitt werden die relevanten Informationen zum autorisierten Benutzer angezeigt, z. B. Identität, Autorisierungsprofil, Autorisierungsrichtlinie und Status.

									Refresh	Never	Show Latest 20	records • Within	Las	it 24 hours -	
🗘 Refresh 🔹 🗘 Reset Repeat Counts 🕹 Export To 🗝														🔻 Filter 🕶 🗘 🗸	,
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorization Pro	Posture St	IP Address		Network Device	
×		-			Identity	Endpoint ID	Endpoint Profi	Authentication	Authorization	Authorization Profiles	Posture Statu:	IP Address	٠	Network Device	
	Jun 14, 2020 07:44:59.975 AM	0	o	0	_585b5291f01484dfd1	00:50:56:A0:D6:97	Windows10	Default	Anyconnect	Full Access	Compliant	10.197.164.7			
	Jun 14, 2020 07:44:59.975 AM		0			10.197.243.143			Anyconnect	Full Access	Compliant			ASA	
	Jun 14, 2020 07:44:59.975 AM	~	0		#ACSACL#-IP-PERMI									ASA	
	Jun 14, 2020 07:44:34.963 AM	2	0		#ACSACL#-IP-Posture									ASA	
	Jun 14, 2020 07:44:34.958 AM	~	Q		_585b5291f01484dfd1	00:50:56:A0:D6:97	Windows10	Default	Default >> A	Posture Redirect	Pending			ASA	

Hinweis: Weitere Informationen zur Statusüberprüfung auf der ISE finden Sie in der folgenden Dokumentation:

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-iseposture-over-anyconnect-remote-acces.html#anc7

Um den Authentifizierungsstatus auf dem Duo Admin Portal zu überprüfen, klicken Sie auf "Reports" auf der linken Seite des Admin Panels, das das Authentifizierungsprotokoll anzeigt.

Weitere Informationen: https://duo.com/docs/administration#reports

Um die Debug-Protokollierung für Duo Access Gateway anzuzeigen, verwenden Sie den folgenden Link:

https://help.duo.com/s/article/1623?language=en_US

Benutzerfreundlichkeit



Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Hinweis: Lesen Sie den Artikel <u>Important Information on Debug Commands</u> (Wichtige Informationen zu Debug-Befehlen), bevor Sie debug-Befehle verwenden.

Vorsicht: Auf der ASA können Sie verschiedene Debug-Ebenen festlegen. Standardmäßig wird Ebene 1 verwendet. Wenn Sie die Debug-Ebene ändern, kann die Ausführlichkeit der Debugs zunehmen. Gehen Sie dabei besonders in Produktionsumgebungen vorsichtig vor.

Bei den meisten SAML-Fehlerbehebungen kommt es zu Fehlkonfigurationen, die durch Überprüfen der SAML-Konfiguration oder durch Ausführen von Debugs ermittelt werden können. "debug webvpn saml 255" kann verwendet werden, um die meisten Probleme zu beheben. In Szenarien, in denen dieses Debuggen keine nützlichen Informationen liefert, können jedoch zusätzliche Debugs ausgeführt werden:

debug webvpn 255 debug webvpn anyconnect 255 debug webvpn session 255 debug webvpn request 255

Verwenden Sie zur Behebung von Authentifizierungs- und Autorisierungsproblemen auf ASA die folgenden Debug-Befehle:

debug radius all debug aaa authentication debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to

posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)

Hinweis: Detaillierte Informationen zum Statusverlauf und zur Fehlerbehebung bei AnyConnect und ISE finden Sie unter dem folgenden Link: <u>ISE Posture Style Comparison for Pre and Post 2.2</u>

So interpretieren Sie Duo Access Gateway-Debug-Protokolle und beheben Fehler <u>https://help.duo.com/s/article/5016?language=en_US</u>

Zugehörige Informationen

https://www.youtube.com/watch?v=W6bE2GTU0Is&

https://duo.com/docs/cisco#asa-ssl-vpn-using-saml https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-postureover-anyconnect-remote-acces.html#anc0

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.