使用CSD、DAP和AnyConnect 4.0配置ASA VPN安全狀態

目錄

簡介 必要條件 需求 採用元件 設定 網路圖表 **ASA** 步驟1.基本SSL VPN配置 步驟2. CSD安裝 步驟3. DAP策略 ISE 驗證 CSD和AnyConnect調配 安全狀態的AnvConnect VPN會話 — 不相容 安全狀態的AnyConnect VPN會話 — 相容 疑難排解 AnyConnect DART 相關資訊

簡介

本文檔介紹如何執行在自適應安全裝置(ASA)上終止的遠端VPN會話的狀態。 ASA使用帶有 HostScan模組的Cisco Secure Desktop(CSD)在本地執行安全狀態。建立VPN會話後,允許符合的 站點進行完全網路訪問,而不符合的站點進行有限的網路訪問。

此外,還介紹了CSD和AnyConnect 4.0調配流程。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco ASA VPN配置
- Cisco AnyConnect Security Mobility Solution 遠端存取

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Microsoft Windows 7
- Cisco ASA 9.3版或更高版本
- Cisco Identity Services Engine(ISE)軟體1.3版及更新版本
- Cisco AnyConnect Security Mobility Solution 4.0及更新版本
- CSD 3.6版或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



公司政策如下:

•具有檔案c:\test.txt(相容)的遠端VPN使用者必須擁有對公司內部資源的完全網路訪問許可權

沒有檔案c:\test.txt(不符合)的遠端VPN使用者必須對公司內部資源具有有限的網路訪問許可權:僅提供對補救伺服器1.1.1的訪問。

檔案存在是最簡單的示例。可以使用任何其他條件(防病毒、反間諜軟體、進程、應用程式、登錄 檔)。

流程如下:

• 遠端使用者未安裝AnyConnect。他們訪問CSD和AnyConnect調配的ASA網頁(以及VPN配置 檔案)

- 通過AnyConnect進行連線後,允許不合規使用者訪問有限網路。已匹配名為FileNotExists的動態訪問策略(DAP)。
- 使用者執行修復(手動安裝檔案c:\test.txt),然後再次與AnyConnect連線。這一次,將提供完整的網路訪問(匹配名為FileExists的DAP策略)。

可以在終端上手動安裝HostScan模組。示例檔案(hostscan-win-4.0.00051-pre-deploy-k9.msi)在 Cisco Connection Online(CCO)上共用。 但是,也可以從ASA推送它。HostScan是可以從ASA調配 的CSD的一部分。第二個方法在本示例中使用。

對於舊版AnyConnect(3.1及更低版本),CCO上有一個單獨的軟體包(例如

:hostscan_3.1.06073-k9.pkg),可以單獨在ASA上配置和調配(使用**csd hostscan image**命令) — 但是對於AnyConnect版本4.0,該選項不再存在。

ASA

步驟1.基本SSL VPN配置

ASA預配置了基本遠端VPN訪問(安全套接字層(SSL)):

webvpn enable outside no anyconnect-essentials anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1 anyconnect enable tunnel-group-list enable group-policy AllProtocols internal group-policy AllProtocols attributes vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless tunnel-group TAC type remote-access tunnel-group TAC general-attributes address-pool POOL authentication-server-group ISE3 default-group-policy AllProtocols tunnel-group TAC webvpn-attributes group-alias TAC enable ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0 aaa-server ISE3 protocol radius aaa-server ISE3 (inside) host 10.1.1.100 key ***** 已下載並使用AnyConnect軟體包。

步驟2. CSD安裝

後續配置使用自適應安全裝置管理器(ASDM)執行。CSD軟體包需要下載以快閃記憶體,並從配置 中獲得參考,如圖所示。

Home 😪 Configuration 📴 Monitoria	ing 🔚 Save 🔇 Refresh 🔇 Back 🜔 Forward 🢡 Help	
Device List 🗗 🕂 🗡	Configuration > Remote Access VPN > Secure Desktop Manager > Setup	
 Add Delete	Secure Desktop Image Update Cisco Secure Desktop. Location: disk0:/csd_3.6.6249-k9.pkg Bro	wse Flash Upload Uninstall
192.168.111.10:444 Remote Access VPN Introduction Network (Clent) Access Clentless SSL VPN Access AAA/Local Users AAA/Local Users AAA/Local Users Global Settings Global Settings Secure Desktop Manager Secure Desktop Customization Kost Scan		

如果不啟用Secure Desktop,則無法在DAP策略中使用CSD屬性,如圖所示。

Tal Add Endpo	int Attribute		8
Endpoint Attrib	bute Type: File	*	
Posture Status	s: 💻 🖵		
	🔁 Warning		
	Â	Cisco Secure Desktop (CSD) is not enabled. CSD must be enabled to configure File endpoint attributes. To enable CSD, go to Configuration > Remote Access VPN >Secure Desktop Manager > Setup.	
		ОК	
		OK Cancel Help	

啟用CSD後,安全案頭管理器下會顯示多個選項。

附註:請注意,其中有些已棄用。有關不推薦使用的功能的更多資訊,請參閱:<u>安全案頭</u> (Vault)、快取清理器、按鍵記錄器檢測和主機模擬檢測的功能棄用通知

仍完全支援HostScan,新增新的基本HostScan規則。如圖所示,**c:\test.txt**的存在已得到驗證。

🔥 Home 🦓 Configuration 📴 Monitorin	19 🔚 Save 🔇 Refresh 🔇 Back 🔇	Forward 🦻 Help		CISCO
Device List ⊡ ⊕ ×	Configuration > Remote Access VPII >	Secure Desktop Hanager > Host S	Scan	
Add Delete Connect Find: Go 10.48.67.158:8443 10.48.67.229:444 10.62.97.56:8443 10.62.97.56:8443 10.62.97.56:8443 10.62.97.56:8443 10.62.97.56:8443	Host Scan Create entries to be scanned on the er information can be configured under D Basic Host Scan	ndpoint system. The scanned information marric Access Policies.	n will then be stored in the endpoint attribute	. Access policies using the endpoint
Remote Access VIIII -7 0	Type	ID	Info	
Introduction Network (Client) Access Client) Access Clientiess SSL VPN Access AAA/Local Users Host Scan Image Secure Desktop Manager Secure Desktop Customization Secure Desktop Customization Secure Desktop Customization	Edit File Scan Endpoint ID: 1 File Path: c1\test.txt OK	L Cancel	c:\test.txt	Add V Edit Delete
Device Setup Erewal Go Remote Access VPN	Host Scan Extensions	er 3.6.6259.2 9.2		Configure

此外,還會新增其他高級終端評估規則,如下圖所示。

us			
Vendor	Product	Note	Add
Symantec Corp.	Norton AntiVirus 20.x		Delete
Force File System Protection	date days		
nal Firewall			
nal Firewall	Product	Note	Add
nal Firewall Vendor Microsoft Corp.	Product Microsoft Windows Firewall 7	Note Supports firewall rules	Add Delete

該策略檢查是否存在Symantec Norton AntiVirus 20.x和Microsoft Windows Firewall 7。狀態模組 (HostScan)檢查這些值,但不會強制執行(DAP策略不會驗證這一點)。

步驟3. DAP策略

DAP策略負責使用HostScan收集的資料作為條件,並將特定屬性應用到VPN會話。若要從ASDM建 立DAP策略,請導覽至**Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**,如下圖所示。

Home 😪 Configuration 📴 M	onitoring	Save 🧲	Refresh 🔇 Back	🕥 Forward 💡 Help			CISCO
Device List D P	×	Configuration	> Remote Access VPN	I > Clientless SSL VPN Access	> Dynamic Access Policie		
Add Delete S Connect Find: Go 10.48.67.158:8443 10.43.67.229:444 10.62.145.45:8443	• 11	Configure Dynar For IPsec, Any resources a us policies are ma	ic Access Policies Connect Client, Clienties er is authorized to access tched, the ASA will enfor	s SSL VPN, and Cut-Through-Pro s. All policies in the table below ar ce the DftAccessPolicy.	xy sessions, you can configure re evaluated for matching criter	dynamic access policies (DAP) that ion during session establishment.	: define which network When none of the DAP
10.62.97.56:8443 192.168.11.250:444	-	ACL Priority	Name	Network ACL List	Webtype ACL List	Description	Add
Remote Access VPII @	4	0	FileNotExists ElleEvicto	AQL1			Edit
Introduction Network (Clent) Access Clentess SSL VPN Access Connection Profiles Orner tion Profiles Oroup Polices Oroup Polices Advanced Advanced Advanced Access Policies Advanced Access Introduction Assert Deskton Manager	* m	-	DftAccessPolicy				Delete

第一個策略(FileExists)檢查已配置的VPN配置檔案使用的隧道組名稱(為清楚起見,已省略VPN配 置檔案配置)。 然後會執行其他檢查,檢查檔案**c:\test.txt**,如下圖所示。

licy Name: File	Exists					
scription:					ACL Priority: 0	
election Criter Define the AA below and ev specify the lo	ia A and endpoint attribute ery endpoint attribute gical expression text.	utes used to select this ac has been satisfied. These	cess policy. A policy is attributes can be cre	used when a user's ated using the table	authorization attributes match t s below and/or by expanding th	he AAA attribute criter e Advanced option to
AAA Attribu	te Ope	Attributes values •	Add	Endpoint ID	Name/Operation/Value	Add
cisco.tunnelg	roup =	TAC	Edit	file.1	exists = true	Edit
			Delete			Delete
			Delete			Delete
						Logical C
Advanced			-			
ccess/Authori Configure acc group-policy I that are not s	zation Policy Attribute: ess/authorization attri tierarchy. The resultin pecified in DAP).	s butes for this policy. Attri g VPN authorization policy Bookmarks	bute values specified is an aggregation of [Access Method	here will override the DAP attributes, AAA	se values obtained from the AA attributes, and group-policy hie	A system and the rarchy attributes (tho:
Action	Net	work ACL Filters (client)	Access Method	Webture AC	Ellers (clastiass)	Eurotione
Accon				Webtype Ac	c rivers (ciencess)	Functions
				Network ACL	5	
ACL1		-	Add>>			
		Manage				
		manage	Delete			

因此,不會使用預設設定執行任何操作來允許連線。未使用ACL — 提供完全網路訪問。

檔案檢查的詳情載於圖中。

📴 Edit Endpoint	Attribute		×
Endpoint Attribute	e Type: File		
	Exists	Does not exist	
Endpoint ID:	1		
	c:\test.txt		
Last Update:	< -		days
Checksum:	=		
		Compute CRC32 Checksum	
	ок	Cancel Help	

第二個策略(FileNotExists)類似 — 但此時間條件是**如果檔案不存在**,如下圖所示。

efine the AAA and en elow and every endpo pecify the logical expr	dpoint attributes used to select to int attribute has been satisfied. " ession text.	his access policy. A p These attributes car	olicy is used when a user's be created using the tables	authorization attributes match th below and/or by expanding the	e AAA attribute cri Advanced option t
User has ANY of the fo	lowing AAA Attributes values	•	and the following en	dpoint attributes are satisfied.	
AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Ad
isco.tunnelgroup	= TAC	Edit	file.1	exists != true	Ed
		Delete			Dele
					Logica
ess/Authorization Pol onfigure access/autho oup-policy hierarchy. aat are not specified in	cy Attributes prization attributes for this policy. The resulting VPN authorization (DAP).	Attribute values sp policy is an aggregat	ecified here will override tho ion of DAP attributes, AAA	se values obtained from the AAA attributes, and group-policy hiera	system and the archy attributes (th
cess/Authorization Poli configure access/author roup-policy hierarchy. hat are not specified in Port Forwardin Action	cy Attributes prization attributes for this policy. The resulting VPN authorization (n DAP). a Lists Network ACL Filters (clie	Attribute values sp policy is an aggregat Access Met nt)	ecified here will override tho ion of DAP attributes, AAA hod AnyConnect Webtype AC	se values obtained from the AAA attributes, and group-policy hiera AnyConnect Cu L Filters (clientless)	a system and the archy attributes (th stom Attributes Function

結果配置了access-list ACL1。適用於提供有限網路訪問的非合規VPN使用者。

兩個DAP策略都推送了**AnyConnect客戶端**訪問,如下圖所示。

Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action	Netwo	k ACL Filters (client)		Webtype ACL Filters (dientless)	Functions
Port Forv	varding Lists	Bookmarks	Access Method	AnyConnect	AnyConnect Cus	tom Attributes
Access Method	: 🔘 Unchanged					
	AnyConnect Cli	ent				
	Web-Portal					
	Both-default-W	eb-Portal				
	Both-default-A	nyConnect Client				

ISE

ISE用於使用者身份驗證。必須僅配置網路裝置(ASA)和正確的使用者名稱(cisco)。本文未涉及該部分。

驗證

使用本節內容,確認您的組態是否正常運作。

CSD和AnyConnect調配

最初,使用者沒有使用AnyConnect客戶端進行調配。使用者也不符合策略(**檔案c:\test.txt**不存在)。 輸入<u>https://10.62.145.45</u>,系統會立即將使用者重新導向以安裝CSD,如下圖所示。

Cisco	Secure Desktop
WebLaunch Platform Detection - ActiveX - Java Detection - Sun Java - WebLaunch - Access Denied - Critical Error	Using ActiveX for Installation Launching Cisco Secure Desktop. If the software does not start properly, <u>Click here</u> to end the session cleanly.
- Access Denied	

這可以通過Java或ActiveX來實現。安裝CSD後,如圖所示進行報告。

Cisco	Secure Desktop
WebLaunch Platform Detection	System Validated Cisco Secure Desktop successfully validated your system. Success, Reloading, Please wait
 ActiveX Java Detection Sun Java 	
 WebLaunch - Access Denied - Critical Error 	
- Success - Access Denied	Download

然後使用者重新導向以進行驗證,如下圖所示。

Login
Please enter your username and password.
GROUP: TAC USERNAME: PASSWORD:
Login

如果成功,將部署AnyConnect以及配置的配置檔案 — 同樣可以使用ActiveX或Java,如下圖所示。

رازیران AnyC دisco	onnect Secure Mobility Client
NebLaunch	Using ActiveX for Installation
	Launching Cisco AnyConnect Secure Mobility Client.
 Platform Detection 	If the software does not start properly, <u>Click here</u> to end
- ActiveX	AnyConnect Secure Mobility Client Downloader
- Java Detection	Downloading AnyConnect Secure Mobility Client 4.0.00051.
🔄 - Java	Time Left: 9 secs (672.0 KB of 3.34 MB copied)
- Download	
Connected	Cancel
	Help Download

並且,VPN連線已建立,如下圖所示。

cisco AnyConnect Secure Mobility Client						
🔦 WebLaunch	Using ActiveX for Installation Launching Cisco AnyConnect Secure Mobility Client.					
 Platform Detection 	If the software does not start properly, <u>Click here</u> to end the session cleanly.					
- ActiveX	AnyConnect Secure Mobility Client Downloader					
 Java Detection Java 	Please wait while the VPN connection is established					
- Download						
Connected						
	Help Download					

AnyConnect的第一步是執行狀態檢查(HostScan)並將報告傳送到ASA,如下圖所示。

🕥 Cisco AnyConnect Secure Mobility Client 📃 📼 💌							
	PN: osture Assessment: Initiating asav	T		Connect			
Limited Access -	DNS Failure						
\$ (i)					cisco		

然後,AnyConnect驗證並完成VPN會話。

安全狀態的AnyConnect VPN會話 — 不相容

當您使用AnyConnect建立新的VPN會話時,第一步是如螢幕截圖所示的終端安全評估狀態 (HostScan)。然後,進行身份驗證,並建立VPN會話,如圖所示。

🕙 Cisco	AnyConnect	10.62.145.45			
	Please enter	your username and password.			
_	Group:	TAC			
	Username:	cisco			
	Password:	******			
		OK Cancel			
S Cisco	AnyConnec	t Secure Mobility Client 📃 🛛	B		
VPN: Please enter your username and password. asav Connect					
Limite	ed Access - DN	IS Failure			
¢ (i		alialia cisco		

ASA報告已收到HostScan報告:

%ASA-7-716603: Received 4 KB Hostscan data from IP <10.61.87.251> 然後執行使用者身份驗證:

%ASA-6-113004: AAA user authentication Successful : server = 10.62.145.42 : user = cisco 並啟動該VPN會話的授權。啟用「debug dap trace 255」後,會返回有關c:\test.txt檔案存在的資訊

DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.file["1"].exists="false" DAP_TRACE: endpoint.file["1"].exists = "false" DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.file["1"].path="c:\test.txt" DAP_TRACE: endpoint.file["1"].path = "c:\\test.txt"

此外,有關Microsoft Windows防火牆的資訊:

DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].exists="false" DAP_TRACE: endpoint.fw["MSWindowsFW"].exists = "false" DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].description="Microsoft Windows Firewall" DAP_TRACE: endpoint.fw["MSWindowsFW"].description = "Microsoft Windows Firewall" DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].version="7" DAP_TRACE: endpoint.fw["MSWindowsFW"].version = "7" DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].enabled="failed" DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].enabled="failed"

和Symantec AntiVirus(根據之前配置的HostScan Advanced Endpoint Assessment規則)。

因此,DAP策略匹配:

DAP_TRACE: Username: cisco, **Selected DAPs: ,FileNotExists** 該策略強制使用AnyConnect並應用訪問清單ACL1,該清單為使用者提供受限的網路訪問(不符合 公司策略):

endpoint.anyconnect.clientversion = "4.0.00051"; endpoint.anyconnect.platform = "win"; endpoint.anyconnect.devicetype = "innotek GmbH VirtualBox"; endpoint.anyconnect.platformversion = "6.1.7600 "; endpoint.anyconnect.deviceuniqueid = "A1EDD2F14F17803779EB42C281C98DD892F7D34239AECDBB3FEA69D6567B2591"; endpoint.anyconnect.macaddress["0"] = "08-00-27-7f-5f-64"; endpoint.anyconnect.useragent = "AnyConnect Windows 4.0.00051"; 因此,VPN會話為Up,但網路訪問受到限制:

ASAv2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

```
Index : 4
Public IP : 10.61.87.251
          : cisco
Username
Assigned IP : 192.168.1.10
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
          : AnyConnect Premium
License
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx
           : 11432
                                  Bytes Rx : 14709
Pkts Tx
          : 8
                                  Pkts Rx
                                             : 146
Pkts Tx Drop : 0
                                  Pkts Rx Drop : 0
Group Policy : AllProtocols
                                  Tunnel Group : TAC
Login Time : 11:58:54 UTC Fri Dec 26 2014
          : 0h:07m:54s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                  VLAN
                                          : none
Audt Sess ID : 0add006400004000549d4d7e
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 10.61.87.251
Encryption : none
                                  Hashing : none
TCP Src Port : 49514
                                  TCP Dst Port : 443
Auth Mode : userPassword
                              Idle TO Left : 22 Minutes
Idle Time Out: 30 Minutes
Client OS : win
Client OS Ver: 6.1.7600
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx
          : 5716
                                  Bytes Rx : 764
           : 4
                                   Pkts Rx
                                              : 1
Pkts Tx
Pkts Tx Drop : 0
                                   Pkts Rx Drop : 0
SSL-Tunnel:
Tunnel ID : 4.2
Assigned IP : 192.168.1.10
                             Public IP : 10.61.87.251
Hashing : SHA1
Encryption : RC4
Encapsulation: TLSv1.0
                                  TCP Src Port : 49517
                                  Auth Mode : userPassword
TCP Dst Port : 443
                             Idle TO Left : 22 Minutes
Idle Time Out: 30 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx : 5716
                                  Bytes Rx : 2760
           : 4
                                              : 12
Pkts Tx
                                   Pkts Rx
Pkts Tx Drop : 0
                                   Pkts Rx Drop : 0
Filter Name : ACL1
DTLS-Tunnel:
Tunnel ID : 4.3
                              Public IP : 10.61.87.251
Assigned IP : 192.168.1.10
Encryption : AES128
                                  Hashing : SHA1
Encapsulation: DTLSv1.0
                                  UDP Src Port : 52749
                                  Auth Mode : userPassword
UDP Dst Port : 443
                              Idle TO Left : 24 Minutes
 Idle Time Out: 30 Minutes
```

Client OS: WindowsClient Type: DTLS VPN ClientClient Ver: Cisco AnyConnect VPN Agent for Windows 4.0.00051Bytes Tx: 0Bytes Tx: 0Pkts Tx: 0Pkts Tx: 0Pkts Tx Drop: 0Filter Name: ACL1

ASAv2# show access-list ACL1 access-list ACL1; 1 elements; name hash: 0xe535f5fe access-list ACL1 line 1 extended permit ip any host 1.1.1.1 (hitcnt=0) 0xe6492cbf

AnyConnect歷史記錄顯示了狀態進程的詳細步驟:

12:57:47	Contacting 10.62.145.45.
12:58:01	Posture Assessment: Required for access
12:58:01	Posture Assessment: Checking for updates
12:58:02	Posture Assessment: Updating
12:58:03	Posture Assessment: Initiating
12:58:13	Posture Assessment: Active
12:58:13	Posture Assessment: Initiating
12:58:37	User credentials entered.
12:58:43	Establishing VPN session
12:58:43	The AnyConnect Downloader is performing update checks
12:58:43	Checking for profile updates
12:58:43	Checking for product updates
12:58:43	Checking for customization updates
12:58:43	Performing any required updates
12:58:43	The AnyConnect Downloader updates have been completed.
12:58:43	Establishing VPN session
12:58:43	Establishing VPN - Initiating connection
12:58:48	Establishing VPN - Examining system
12:58:48	Establishing VPN - Activating VPN adapter
12:58:52	Establishing VPN - Configuring system
12:58:52	Establishing VPN
12:58:52	Connected to 10.62.145.45.

安全狀態的AnyConnect VPN會話 — 相容

建立**c:\test.txt**檔案後,流程相似。啟動新的AnyConnect會話後,日誌將指示檔案的存在:

%ASA-7-734003: DAP: User cisco, Addr 10.61.87.251: Session Attribute endpoint.file["1"].exists="true" %ASA-7-734003: DAP: User cisco, Addr 10.61.87.251: Session Attribute endpoint.file["1"].path="c:\test.txt" 因此使用另一個DAP策略:

DAP_TRACE: Username: cisco, **Selected DAPs: ,FileExists** 該策略不會將任何ACL強制用作網路流量的限制。

且作業階段在沒有任何ACL的情況下為Up(完全網路存取):

: 5 Index : cisco Username Public IP Assigned IP : **192.168.1.10** : 10.61.87.251 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 11432 Bytes Rx : 6298 Pkts Tx : 8 Pkts Rx : 38 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : AllProtocols Tunnel Group : TAC Login Time : 12:10:28 UTC Fri Dec 26 2014 : 0h:00m:17s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0add006400005000549d5034 Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 5.1 Public IP : 10.61.87.251 Encryption : none Hashing : none TCP Src Port : 49549 TCP Dst Port : 443 Auth Mode : userPassword Idle TO Left : 29 Minutes Idle Time Out: 30 Minutes Client OS : win Client OS Ver: 6.1.7600 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051 Bytes Tx : 5716 Bytes Rx : 764 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 5.2 Public IP : 10.61.87.251 Assigned IP : 192.168.1.10 Encryption : RC4 Hashing : SHA1 Encapsulation: TLSv1.0 TCP Src Port : 49552 Auth Mode : userPassword TCP Dst Port : 443 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 4.0.00051 Bytes Tx : 5716 Bytes Rx : 1345 : 4 Pkts Rx : 6 Pkts Tx Pkts Rx Drop : 0 Pkts Tx Drop : 0 DTLS-Tunnel: Tunnel ID : 5.3 Assigned IP : 192.168.1.10 Public IP : 10.61.87.251 Encryption : AES128 Hashing : SHA1 Encapsulation: DTLSv1.0 UDP Src Port : 54417 Auth Mode : userPassword UDP Dst Port : 443 Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051 Bytes Tx : 0 Bytes Rx : 4189 Pkts Tx : 0 Pkts Rx : 31 Pkts Tx Drop : 0 Pkts Rx Drop : 0

13:10:15 Hostscan state idle
13:10:15 Hostscan is waiting for the next scan

附註:對於重新評估,建議使用與ISE整合的狀態模組。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

AnyConnect DART

AnyConnect提供診斷,如下圖所示。

Statistic Route Details Firewall Message History 13:45:00 Contacting asav. 13:45:00 Contacting asav. 13:45:10 Contacting asav. 13:45:12 Posture Assessment: Required for access 13:45:21 Posture Assessment: Required for access 13:45:21 Posture Assessment: Checking for updates 13:45:21 Posture Assessment: Initiating 13:45:21 Posture Assessment: Active 13:45:21 Posture Assessment: Checking for updates 13:45:21 Posture Assessment: Initiating 13:45:21 Posture Assessment: Initiating 13:45:31 Posture Assessment: Initiating 13:45:31 Posture Assessment: Initiating 13:45:31 Posture Assessment: Initiating 13:45:31 Posture Assessment: Initiating 13:45:41 Hostscan state ide 13:45:41 Hostscan state ide 13:45:42 Checking for profile updates 13:45:42 Checking for profile updates 13:45:42 Checking for customization updates 13:45:42 Checking for customization updates 13:45:42 Checking for profile updates 13:45:42 The AnyConnect Downloader updates have been completed. 13:45:42 Establis	9	Cis	co AnyConne	ect Secure I	Mobility Client						×
Virtual Private Network (VPN) Diagnostics Preferences Statistics Route Details Firewall Message History 13:45:00 Contacting asav. 13:45:09 Connection attempt has failed. 13:45:13 Contacting 10.62.145.45. 13:45:21 Posture Assessment: Required for access 13:45:21 Posture Assessment: Checking for updates 13:45:22 Posture Assessment: Initiating 13:45:22 Posture Assessment: Initiating 13:45:31 Posture Assessment: Active 13:45:31 Posture Assessment: Initiating 13:45:35 User ordentials entered. 13:45:41 Hostscan state idle 13:45:41 Hostscan state idle 13:45:42 The AnyConnect Downloader is performing update checks 13:45:42 Establishing VPN session 13:45:42 Checking for product updates 13:45:42 Performing any required updates 13:45:42 Performing any required updates 13:45:47 Establishing VPN session E 13:45:47 Establishing VPN session 13:45:47 Establishing VPN session E 13:45:47 Establishing VPN - Examining system T T T T		، ا د	 :isco	AnyC	connect S	Secu	ire Mobili	ty Clien	t		1
Preferences Statistics Route Details Firewall Message History 13:45:00 Contacting asav. 13:45:09 Connection attempt has failed. 13:45:13 Contacting 10.62.145.45. 13:45:21 Posture Assessment: Required for access 13:45:21 Posture Assessment: Checking for updates 13:45:22 Posture Assessment: Initiating 13:45:21 Posture Assessment: Initiating 13:45:31 Posture Assessment: Initiating 13:45:22 Posture Assessment: Initiating 13:45:35 User credentials entered. 13:45:31 Posture Assessment: Initiating 13:45:45 Hostscan is waiting for the next scan 13:45:42 Establishing VPN session 13:45:42 Checking for profile updates 13:45:42 Checking for profile updates 13:45:42 Checking for customization updates 13:45:42 Checking for customization updates 13:45:42 Performing any required updates 13:45:42 The AnyConnect Downloader updates have been completed. 13:45:47 Establishing VPN - Initiating connection 13:45:47 Establishing VPN - Examining system The AnyConnect Downloader updates have been completed. The AnyConnect Downloader updates have been comp	2		Virtual Pri	vate Net	twork (VPN)				Diagnosti	cs	
13:45:00 Contacting asav. 13:45:09 Connection attempt has failed. 13:45:13 Contacting 10.62.145.45. 13:45:14 Posture Assessment: Required for access 13:45:21 Posture Assessment: Checking for updates 13:45:22 Posture Assessment: Initiating 13:45:31 Posture Assessment: Initiating 13:45:45 User credentials entered. 13:45:45 Hostscan state idle 13:45:41 Hostscan is waiting for the next scan 13:45:42 Establishing VPN session 13:45:42 Checking for profile updates 13:45:42 Checking for customization updates 13:45:42 Performing any required updates 13:45:42 Performing any required updates 13:45:42 The AnyConnect Downloader updates have been completed. 13:			Preferences	Statistics	Route Details F	irewall	Message History				
			$13:45:0\\13:45:1\\13:45:2\\13:45:2\\13:45:2\\13:45:2\\13:45:3\\13:45:3\\13:45:3\\13:45:4\\13:45:5\\13:4$	0 Contact 19 Connect 13 Contact 14 Posture 12 Posture 12 Posture 12 Posture 13 Posture 14 Posture 15 User created 14 Hostsca 14 Hostsca 15 Checkin 12 Checkin 12 Checkin 12 Checkin 12 Checkin 13 Checkin 14 Perform 15 Establis 16 Establis 17 Establis 17 Establis 18 Establis 19 Checkin 10 Checkin 10 Checkin 10 Checkin 11 Checkin 12 Checkin 12 Checkin 13 Checkin 14 Checkin 15 Establis 15 Establis 15 Establis 16 Establis	ting asav. tion attempt has f ting 10.62.145.45 Assessment: Rec Assessment: Che Assessment: Initi Assessment: Initi Assessment: Acti Assessment: Initi edentials entered. Assessment: Initi edentials entered. In state idle an is waiting for th hing VPN session. yConnect Downloa g for profile updai g for profile updai g for customizatio ing any required u yConnect Downloa hing VPN session. hing VPN session. hing VPN - Initiatir hing VPN - Examin	ailed. uired fo cking fo ating ve ating e next s der is p tes n updat updates. ader upd ng conne ing syst	r access r updates can erforming update c es lates have been co ection em	hecks		4 III 4	

收集所有AnyConnect日誌並將其儲存到案頭上的zip檔案。該zip檔案包括Cisco AnyConnect Secure Mobility Client/Anyconnect.txt中的日誌。

它提供有關ASA的資訊,並請求HostScan收集資料:

: 12/26/2014 Date : 12:58:01 Time : Information Type Source : acvpnui Description : Function: ConnectMgr::processResponseString File: .\ConnectMgr.cpp Line: 10286 Invoked Function: ConnectMgr::processResponseString Return Code: 0 (0x0000000) Description: HostScan request detected. 然後,多個其他日誌顯示CSD已安裝。以下是CSD調配和後續的AnyConnect連線以及安全狀態的 示例: CSD detected, launching CSD Posture Assessment: Required for access Gathering CSD version information. Posture Assessment: Checking for updates... CSD version file located Downloading and launching CSD Posture Assessment: Updating... Downloading CSD update CSD Stub located Posture Assessment: Initiating... Launching CSD Initializing CSD Performing CSD prelogin verification. CSD prelogin verification finished with return code 0 Starting CSD system scan. CSD successfully launched Posture Assessment: Active CSD launched, continuing until token is validated. Posture Assessment: Initiating... Checking CSD token for validity Waiting for CSD token validity result

CSD token validity check completed CSD Token is now valid CSD Token validated successfully Authentication succeeded Establishing VPN session...

ASA和AnyConnect之間的通訊已最佳化,ASA請求僅執行特定檢查 — AnyConnect將下載其他資料 以便執行該檢查(例如特定防病毒驗證)。

當您使用TAC開啟案例時,請附上Dart日誌以及ASA中的「show tech」和「debug dap trace 255」 。

相關資訊

- 配置主機掃描和狀態模組 Cisco AnyConnect安全移動客戶端管理員指南
- <u>思科ISE上的終端安全評估服務配置指南</u>
- <u>思科ISE 1.3管理員指南</u>
- <u>技術支援與文件 Cisco Systems</u>