Installeer en configureren AnyConnect NVM 4.7.x of hoger en verwante Splunk Enterprisecomponenten voor CESA

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Overzicht van implementaties Achtergrondinformatie Cisco AnyConnect Secure Mobility Client - meer dan VPN Internet Protocol Flow Information Exporteren (IPFIX) **IPFIX NVM Collector** Splunk Enterprise Topologie Configureren Ondersteuning van DTLS certificaatvereisten Standalone AnyConnect NVM module AnyConnect NVM-clientprofiel NVM-clientprofiel configureren via ASDM NVM-clientprofiel configureren via AnyConnect Profile Editor Configuratie van WebDeployment op Cisco ASA Configuratie van Web-Plaatsing op Cisco ISE **Trusted Network Detectie** implementeren Stap 1. Configureer de NVM via Cisco ASA/ISE Stap 2. Stel IPFIX Collector Component in (AnyConnect NVM Collector) Hoe installeert u de Collector? **Ondersteuning van DTLS** Stap 3. Stel Splunk in met Cisco NVM App (CESA Dashboard) en TA Add-On voor Splunk. Installeren UDP-ingangen inschakelen met behulp van Splunk Management UI Verifiëren AnyConnect NVM-installatie valideren Valideren van Collector status als actief Splunk valideren - AnyConnect NVM CESA Dashboard PacketFlow Flow-sjablonen Problemen oplossen

AnyConnect-client (NVM-module) AnyConnect NVM - niet rapporteren aan de Collector - CFLOW-datapakketten blijven geen eindpunt achter Trusted Network Detection (TND) AnyConnect diagnostiek en rapportage-tools (DART) Collector (op Linux/Docker machine - all-in-one of standalone) Splunk Console (NVM Dashboard) geeft geen gegevens weer AnvConnect-client Verzamelbak Vaak gestelde vragen (veelgestelde vragen) 1. Hoe kunt u gegevens van een willekeurige NVM naar meerdere bestemmingen sturen? 2. Waar slaat u het certificaatmodel op voor AnyConnect NVM DTLS? XML-bestandsnamen Collector (anyconnect NVM) Aanbevolen release AnyConnect 4.9.0086 nieuwe functies Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de Cisco AnyConnect Network Visibility Module (NVM) op een eindgebruikersysteem kunt installeren en configureren met AnyConnect 4.7.x of hoger en hoe u de bijbehorende Splunk Enterprise-onderdelen en NVM Collector kunt installeren en configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AnyConnect 4.7.x of hoger met NVM
- AnyConnect-licenties
- ASDM 7.5.1 of hoger
- Bekendheid met Splunk Enterprise en hoe u Splunk-apps en add-ons kunt installeren

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco AnyConnect Security Mobility Client 4.7.x of hoger
- Cisco AnyConnect-profieleditor
- Cisco adaptieve security applicatie (ASA), versie 9.5.2
- Cisco Adaptieve Security Devices Manager (ASDM), versie 7.5.1

- Splunk Enterprise 7.x of hoger (geïnstalleerd als all-in-one op een ondersteunde linux, bij voorkeur CentOS)
- Alle ondersteunde linux-installatie als een verzamelaarsapparaat (de verzamelaar kan ook op dezelfde server draaien, raadpleeg <u>cs.co/cesa-pov</u> voor meer informatie)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

- Voor een compleet overzicht van POV of CESA met Splunk gelieve te verwijzen naar <u>cs.co/cesa-pov</u>
- Voor een gids naar CESA NVM Dashboard op Splunk http://cs.co/cesa-guide
- Raadpleeg voor meer informatie over de oplossing <u>www.cisco.com/go/cesa</u>.

De bestanddelen van de oplossing zijn:

- Cisco AnyConnect Secure Mobility Client met Network Visibility Module (NVM) ingeschakeld
- <u>Cisco AnyConnect Network Visibility Module-app (NVM) voor Splunk</u>
- <u>Cisco NVM Technology Add-on voor Splunk</u>
- NVM Collector (gebundeld in een zip-bestand met de NVM TA Add-on)

Overzicht van implementaties

Dit is een overzicht op hoog niveau van implementatie in zijn eenvoudigste vorm. Dit is een all-inone configuratie die draait op 64-bits Linux.

Dit is hoe de meeste demonstraties worden opgezet en ook nuttig is in een kleine productieinstallatie.



Dit is een uitgebreidere reeks opties die beschikbaar zijn voor plaatsing. Meestal wordt een productie-instelling gedistribueerd en heeft u verschillende knooppunten voor de onderneming.



Achtergrondinformatie

De Cisco AnyConnect Network Visibility Module biedt een continue feed met hoge-eindpunten telemetrie. NVM stelt organisaties in staat om endpoints en gebruikersgedrag op hun netwerk te zien, verzamelt stromen vanuit endpoints aan en buiten de ruimte, samen met waardevolle contexten zoals gebruikers, toepassingen, apparaten, locaties en bestemmingen. Splunk Enterprise gebruikt de telemetrie en biedt de analytische mogelijkheden en rapporten.

Deze technologie is een configuratievoorbeeld voor AnyConnect NVM met Splunk Enterprise als onderdeel van de nieuwe <u>CESA-</u>oplossing.

Cisco AnyConnect Secure Mobility Client - meer dan VPN

Cisco AnyConnect is een eengemaakte agent die meerdere beveiligingsservices levert om de onderneming te beschermen. AnyConnect wordt meestal gebruikt als een VPN-client voor ondernemingen, maar ondersteunt ook extra modules die rekening houden met verschillende aspecten van de bedrijfsbeveiliging. De extra modules maken veiligheidskenmerken zoals beoordeling van de positie, web veiligheid, malware bescherming, netwerkzichtbaarheid en meer mogelijk.

Deze technologie gaat over Network Visibility Module (NVM), die geïntegreerd is met Cisco AnyConnect om beheerders de mogelijkheid te bieden om internetgebruik te bewaken.

Raadpleeg voor meer informatie over Cisco AnyConnect <u>Cisco AnyConnect Secure Mobility Client</u> <u>Administrator Guide, release 4.7</u>

Internet Protocol Flow Information Exporteren (IPFIX)

IPFIX is een IETF-protocol om een norm te definiëren voor het exporteren van IP-stroominformatie voor verschillende doeleinden, zoals boekhouding/controle/beveiliging. IPFIX is gebaseerd op Cisco NetFlow Protocol v9, alhoewel niet direct compatibel. <u>Cisco nvzFlow</u> is een protocolspecificatie die is gebaseerd op het IPFIX-protocol. Door ontwerp, is IPFIX een

uitbreidbaar protocol dat toelaat om nieuwe parameters te definiëren om informatie over te brengen. Cisco nvzFlow-protocol breidt de IPFIX-standaard uit en definieert nieuwe informatieelementen evenals een standaardset IPFIX-sjablonen die worden verzonden als onderdeel van de telematica die door AnyConnect NVM wordt gebruikt.

Raadpleeg voor meer informatie over IPFIX rfc5101,rfc7011,rfc7012,rfc7013,rfc7014,rfc7015.

IPFIX NVM Collector

Voor meer informatie over de http://cs.co/nvm-collector

- Een verzamelaar is een server die IPFIX-gegevens ontvangt en opslaat. Het kan deze gegevens dan aan Splunk geven.
- Cisco biedt een verzamelaar die specifiek is ontworpen voor het nvzFlow-protocol en wordt gebundeld met de Splunk App (NVM TA Add-On).
- De verzamelaar kan in hetzelfde vak (all-in-one) met de Splunk-server worden geïnstalleerd. Op de vrachtwagen. Of in een standalone linux doos.

Splunk Enterprise

Splunk Enterprise is een krachtig instrument dat diagnostische gegevens verzamelt en analyseert om betekenisvolle informatie te geven over de IT-infrastructuur. Het biedt een one-stop locatie voor beheerders om gegevens te verzamelen die van cruciaal belang zijn voor het begrip van de gezondheid van het netwerk.

Splunk is een partner van Cisco en de <u>CESA</u> oplossing werd gemaakt in samenwerking met hen.

Topologie



IP-adresconventies in deze technologie:

IP-adres van verzamelaar: 192.0.2.123

IP-adres splitsen: 192.0.2.113

Configureren

Dit deel heeft betrekking op de configuratie van Cisco NVM-onderdelen.

Voor een overzicht van de implementatie van AnyConnect NVM en het configuratie-profiel wordt ook verwezen naar <u>Hoe de AnyConnect Network Visibility Module te implementeren</u>

Ondersteuning van DTLS

NVM kan nu worden ingesteld om gegevens via DTLS veilig naar de verzamelaar te sturen. Deze

modus kan worden ingesteld in de NVM Profile Editor. Wanneer het aanvinkvakje "Secure" is ingeschakeld, gebruikt NVM DTLS als transport. Voor de DTLS-verbinding die door moet gaan, dient het DTLS-servercertificaat (collector) op het eindpunt te worden vertrouwd. Onvertrouwde certificaten worden in stilte afgewezen. DTLS 1.2 is de minimale ondersteunde versie. De verzamelaar als deel van CESA Splunk App v3.1.2+ is vereist voor DTLS-ondersteuning. De verzamelaar werkt alleen in één modus, veilig of onveilig.

certificaatvereisten

- Het Collector attest moet worden vertrouwd door de klant (moet ervoor zorgen dat de certificeringsketen betrouwbaar is), er is geen configuratie op AnyConnect.
- Het certificaat moet in PEM-formaat zijn.
- ondersteunt geen wachtwoord voor certificaat en toets (Cisco ISE interne CA vereist één)
- Elk certificaat kan op de verzamelaar worden gebruikt zolang de AnyConnectclientmachine het vertrouwt (interne PKI, bekend, enz.).
- Nadat het configuratiebestand is bijgewerkt, moet de NVM-service opnieuw worden gestart (voor één client testen). Voor profielen die vanaf ISE/ASA zijn geduwd, moet de verbinding met het netwerk worden verbroken of opnieuw worden aangesloten.
- AC NVM Profile Collector Configuration moet IP of FQDN zijn. Dit hangt af van het gebruik in de GN van het certificaat. FQDN wordt altijd geprefereerd in het geval van IP adresveranderingen. Als u een IP-adres gebruikt, dan moet het verzamelaarscertificaat CN of SAN ook dat IP hebben. Als FQDN als GN in het certificaat staat, moet het NVMprofiel dezelfde FQDN als een verzamelaar hebben.

AnyConnect Configuration (4.9.3043 en hoger) - zie Collector info

NVM-profiel is er een nieuw selectieteken onder de naam Secure voor verzamelaars IP/poort.

NVM Pr	ofile
Profile:	Untitled
	Collector Configuration IP Address/FQDN
	Collector Configuration IP Address/FQDN Port

Standalone AnyConnect NVM module

Hiervoor is AnyConnect 4.8.01090 of hoger nodig - AnyConnect Admin Guide voor NVM

Raadpleeg ook de standalone handleiding - <u>Hoe u de AnyConnect-netwerkzichtbaarheidsmodule</u> <u>implementeert</u>

Voor degenen die geen AnyConnect-implementatie hebben of een andere VPN-oplossing

gebruiken, kunt u het NVM-standalone pakket voor uw NVM-behoeften installeren. Dit pakket werkt onafhankelijk, maar biedt hetzelfde niveau van stroomverzameling vanuit een eindpunt als de bestaande AnyConnect NVM-oplossing. Als u de standalone NVM installeert, wijzen de actieve processen (zoals de activiteitsmonitor op macOS) het gebruik aan.

Standalone NVM is ingesteld met de<u>NVM Profile Editor</u>, en Trusted Network Detection (TND)configuratie is verplicht. Met behulp van de TND-configuratie bepaalt NVM of het eindpunt op het bedrijfsnetwerk ligt en past zij vervolgens het juiste beleid toe.

Problemen oplossen en registreren worden nog steeds uitgevoerd door AnyConnect DART, die vanaf het AnyConnect-pakket kan worden geïnstalleerd.

Voorafgaand aan de zelfstandige, moest de Core VPN module geïnstalleerd zijn om voordeel te halen uit Trusted Network Detection, wat er ook toe leidde dat de gebruiker de kern VPN-bundel in UI zag, die de eindgebruikers in verwarring kan brengen, vooral als zij een andere verkoper VPN-oplossing gebruiken.

Wanneer u de stand-alone gebruikt, gebruikt u het core VPN-profiel niet om TND te configureren. Het NVM-profiel kan nu rechtstreeks voor TND worden ingesteld.

		dc	oud-rtp-web-4.cisco.com		C	0 1
0 0 🚼 🛆 O	E 🖸 📓 📾 📥 🚯	Cisco dCloud	ad1	wkst3	wkst2	wkst4 +
AnyConnect Profile Editor -	VPN	_ O X	AnyConnect Profile Ed	itor - NVM Profile		
File Help			File Help			
VPN - @ Preferences (Part 1)	Preferences (Part 2)		NVM Profile Profile: Untitled			Desktop
Preferences (Part 2)	Profile: Untitled		Profile: Ontided			
Certificate Pinning	Disable Automatic Certificate Selection	User Controllable	Collector	Configuration	Cache Configuration	
Certificate Enrolment	Proxy Settings Native	User Controllable	IP Addre	ss/FQDN	Max Size 50	MB
Server List	Public Proxy Server Address:		Port		Max Duration	days
	Allow Local Proxy Connections	ddress and Port here. Example:10.86.125.33:8080				
	Enable Optimal Gateway Selection	🔽 User Controllable	Periode	Template Report 1440 mins		
	Suspension Time Threshold (hours)	4		Note: Valid range: Smins	24hrs(1440mins).	
	Performance Improvement Threshold (%)	20	, Periode	Flow Report		
	Automatic VPN Policy Trusted Network Policy	Dimment	Acces	ation Interval 5 seconds		
	Untrusted Network Policy	Connect				
	Trusted DNS Domains		Throttle	Note: Valid range: 12 - 20	48. To disable: 0.	
	Trusted DNS Servers		Collecti	on Mode All Networks	¥	
	Note: adding all DNS servers in use is recomme	nded with Trusted Network Detection	Collecti	on Criteria T Broadcast packets	_	
	Trusted Servers @ https:// <server>[:<port>]</port></server>			Multicast packets		
	https://	Add	; Data C	ollection Policy	Add	
		Delete			Edt	
					Desete	
				manufacture Confirm 1		
			Inusceo	Network Detection Corrigure	—	
	Certificate Hash:	Set	If much such		(This is a True to distant	and Defection much
	E there on	(More Information)	If not usin	ig AnyConnect for	VPN then Trusted Netw	Ork Detection must
	E Alexe VSN Disconnect		De config	ured here in the loft	wiprofile otherwise it i	S configured as part
	Connect Failure Policy	Closed	Of the VP.	<u>prome on the left</u>	under-Automatic VPN	Policy
	-		1			
	() Help				() Help	
🎝 Start 🕌 🗾	😫 😼 🚰					🍖 💁 🖾 😘 🚺 🛞 🏱 👫 5:18 PM

AnyConnect NVM-clientprofiel

AnyConnect NVM configuratie wordt opgeslagen in een XML-bestand met informatie over het IPadres en poortnummer van de verzamelaar, samen met andere informatie. Het IP-adres van de verzamelaar en een poortnummer moeten correct worden ingesteld in het NVM-clientprofiel.

Voor een correcte werking van de NVM-module moet het XML-bestand in deze map worden geplaatst:

- Voor Windows 7 en hoger: %ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure
 Mobility Client\NVM
- Voor Mac OSX: /opt/cisco/anyconnect/nvm

Als het profiel op Cisco ASA/Identity Services Engine (ISE) aanwezig is, wordt het samen met AnyConnect NVM-implementatie automatisch ingezet.

XML-profielvoorbeeld:

<?xml version="1.0" encoding="UTF-8"?>
-<NVMProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="NVMProfile.xsd">
-<CollectorConfiguration>
<CollectorConfiguration>
<CollectorIP>192.0.2.123</CollectorIP>
<Port>2055</Port>
</CollectorConfiguration>
<Anonymize>false</Anonymize>
<CollectionMode>all</CollectionMode>
</NVMProfile>

Met deze tools kan NVM-profiel worden gemaakt:

- Cisco ASDM
- AnyConnect-profiel-editor
- Identity Services Engine

NVM-clientprofiel configureren via ASDM

Deze methode is te verkiezen als AnyConnect NVM wordt ingezet via Cisco ASA.

1. Navigeer in op configuratie > Toegang tot VPN > Toegang tot netwerk (client) > AnyConnectclientprofiel verwijderen.

2. Klik op Add, zoals in de afbeelding.

Remote Access VPN a P	Configuration > Remote Acce	ss VPN > Network (Client) Access > AnyCor	mect Client Profile						
 Introduction Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localiza AnyConnect Client Profile AnyConnect Client Profile Group Policies IPsec(IKEV2) Connection Profiles Secure Mobility Solution Advanced Clientlese SSL VPN Access AAA/Local Users Secure Mobility Solution Clientlese SSL VPN Access AAA/Local Users Secure Mobility Solution Advanced Clientlese SSL VPN Access AAA/Local Users Detrificate Manager Detrof Server DHCP Server DHCP Server Advanced 	This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device. The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.								
	Profile Name	Profile Usage	Group Policy Profile Location						
III Device Setup									
Remote Access VPN									
Site-to-Site VPN									
Device Management									
*		(Apply Reset						

3. Geef het profiel een naam. Selecteer in profiel gebruik de optie Netwerkzichtbaarheidsprofiel.

4. Wijs het toe aan het groepsbeleid dat door AnyConnect-gebruikers wordt gebruikt en klik op **OK**, zoals in de afbeelding.

Remote Access VPN a P	Configuration > Remote Acces	s VPN > Network (Client) Access > AnyCor	inect Client Profile			
Introduction Introduction Introduction Introduction Introduction Introduction Introduction AnyConnect Customization/Localiza Introduction Introduction AnyConnect Client Software Comparis Access Policies Group Policies Group Policies	This panel is used to manage An select the 'Add' button to add a The profile Usage field is introdu	yConnect Client Profiles and perform group assistive yrofile. Pressing the Import or Export button ced with the Secure Mobility Solution. This field up Policy 👔 Delete 💽 Import 👼 Export 🚳 Va	gnment for AnyConnect version 2. is for upload and download of cl contains different profile usage in slidate	.5 or later. You can select a pr lent profiles between local ma AnyConnect version 3.0 and	rofile to edit, change group or to delete. You can achine and device. later.	
 IPsec(IKEv1) Connection Profiles IPsec(IKEv2) Connection Profiles 	Profile Name	Profile Usage	Group Policy		Profile Location	
Address Assignment Address Assignment Address Assignment Address SSL VPI Access AAA/Local Users AAA/Local Users Centificate Management Daguage Localization DHCP Server DHCP Server Advanced	Add AnyCo Profile Name Profile Usage Enter a devic created if it Profile Locati Group Policy	nnect Client Profile IVM_policy INEWOrk Visibility Service Profile See file path for an xml file, le. disk0:/ac_profile. T Joes not exist. Ion disk0:/nvm_policy.nvmsp GroupPolicy_anyconnect Enable/ "Means On VISM" for relacted and	The file will be automatically	Browse Flash Upload		
		OK Cance	Help Apply Reset			

5. Klik op Bewerken om het nieuwe beleid te maken, zoals in de afbeelding.

Remote Access VPN 07 9	Configuration > Remote Acce	ss VPN > Network (Client) Access > AnyConnect	Client Profile		
Introduction I	This panel is used to manage A restect the 'Add' button to add a The profile Usage field is introd	nyConnect Client Profiles and perform group assignment new profile. Pressing the Import or Export button is for luced with the Secure Mobility Solution. This field contain roup Policy Delete Data Import Science Science Of Validate	t for AnyConnect version 2.5 or later. You can : upload and download of client profiles betwee is different profile usage in AnyConnect versio	select a profile to edit, change group or to delete. You can n local machine and device. n 3.0 and later.	
 IPsec(IKEv2) Connection Profiles IPsec(IKEv2) Connection Profiles 	Profile Name	Profile Usage	Group Policy	Profile Location	
Secure Mobility Solution Address Assignment	NVM_policy	Network Visibility Service Profile	GroupPolicy_anyconnect	disk0:/nvm_policy.nvmsp	
Secure Desktop Manager					
A Device Setup					
Firewall					
Remote Access VPN					
Site-to-Site VPN					
Device Management					
1	•	A	pply Reset		

6. Voer de informatie in over het IP-adres en het poortnummer van de verzamelaar en klik op OK.

7. Klik nu op **Toepassen**, zoals in de afbeelding.

Remote Access VPN B P	AnyConnect Client Profile Edit	or - NVM_policy	X	
Introduction Network (Client) Access AnyConnect Connection Profiles	Profile: NVM_policy		About	or to delete. You can
AnyConnect Customization/Localiza AnyConnect Client Profile AnyConnect Client Software	NVM Profile			
Pynamic Access Policies Group Policies Prec(IKEV1) Connection Profiles Psec(IKEV2) Connection Profiles Secure Mobility Solution	Collector Configuration			
Address Assignment Advanced	IP Address/FQDN	192.0.2.123		2
Clientless SSL VPN Access AAA/Local Users Secure Desktop Manager Secure Desktop Manager Secure Contracter Management	Port	2055		
B Language Localization Load Balancing DHCP Server DHCP Server DNS DNS	User Anonymization	False •		
	Collection Mode	All Networks		
<				
S Device Setup				
🚮 Firewall				
Remote Access VPN		OK Cancel Help		
Site-to-Site VPN				
Device Management				
20		Apply Reset		

NVM-clientprofiel configureren via AnyConnect Profile Editor

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect49/administratio n/guide/b_AnyConnect_Administrator_Guide_4-9/anyconnect-profile-editor.html#ID-1430-00000061 Dit is een zelfstandige tool die beschikbaar is op Cisco.com. Deze methode is te verkiezen als AnyConnect NVM wordt uitgevoerd via Cisco ISE. Het NVM-profiel dat met dit gereedschap is gemaakt, kan naar Cisco ISE worden geüpload of rechtstreeks naar endpoints worden gekopieerd.

AnyConn	ect Profile Editor - NVM Prof	ïle	- • ×
File Help		И	
NVM Pro	ofile		
Profile:	Untitled		
	Collector Configuration		
	IP Address/FQDN	192.0.2.123	
	Port	2055	
	User Anonymization	False	
	Collection Mode	All Networks	
		() Help	

Raadpleeg voor meer informatie over AnyConnect Profile Editor het volgende:

De AnyConnect-profiel-editor

Configuratie van WebDeployment op Cisco ASA

Deze technologie gaat ervan uit dat AnyConnect al op de ASA is geconfigureerd en dat alleen de configuratie van de NVM-module moet worden toegevoegd. Raadpleeg voor meer informatie over ASA AnyConnect-configuratie:

ASDM Boek 3: Cisco ASA Series 5000 Series VPN ASDM-configuratiegids, 7.5

Voer de volgende stappen uit om AnyConnect NVM-module op Cisco ASA in te schakelen:

1. Navigeer naar Configuration > Remote Access VPN > Network (Client) Access > Group Policy.

2. Selecteer het betreffende groepsbeleid en klik op Bewerken, zoals in de afbeelding.

Remote Access VPN d P	Configuration > Remote Access V	PN > Network (Client) Access >	Group Policies	
Introduction Network (Client) Access B AnyConnect Connection Profiles AnyConnect Customization/Localiza AnyConnect Client Profile AnyConnect Client Software	Manage VPN group policies.A VPN group policy information is reference To enforce authorization attributes & Add - C Edit Delete X A	group is a collection of user-oriented ed by VPN connection profiles and u from an LDAP server you must use a ssign	authorization attribute/value pairs that may be stored in ser accounts.	iternally on the device or externally on a RADIUS/LDAP server. The
Group Policies IPsec(IKEv1) Connection Profiles	Name	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To
- Secure Mobility Solution	GroupPolicy_anyconnect	Internal	ssi-client	anyconnect
🕀 🌆 Address Assignment	splitdns	Internal	ssl-client	splitdns
AAA/Local Users AAA/Local Users Hots Scan Image Cartificate Manager Load Balancing Del Desrver DNS Cartificate Managerent Data Balancing DNS Cartificate Managerent DNS Cartificate Managerent DNS	unarproixy (system berdan)	2000 HOI	ineva, ineva, iser unenness, izuprijoec	Deraultovar og, beraultiztist og, beraultophana og p
• [
Device Setup				
🞲 Firewall				
Remote Access VPN				
Site-to-Site VPN				
🖏 🖭	Find:	🔿 🥅 Match Case		
Device Management		S		
» •			Apply Reset	

3. In de pop-up met groepsbeleid, navigeer naar Advanced > AnyConnect Client.

4. Optionele clientmodules uitvouwen om te downloaden en Any-connect netwerkzichtbaarheid te selecteren.

5. Klik op **OK** en pas wijzigingen toe.

ieneral	Keep Installer on Client System:	🔽 Inherit	O Yes	O No		
dvanced	Datagram Transport Layer Security (DTLS):	🔽 Inherit	🔿 Enable	🔘 Disable		
-Split Tunneling Browser Proxy	DTLS Compression:	🔽 Inherit) Enable	🔿 Disable		
B AnyConnect Client B IPsec(IKEv1) Client	SSL Compression:	📝 Inherit	🔿 Deflate	© LZS	🔘 Disable	
	Ignore Don't Fragment(DF) Bit:	🔽 Inherit	🔘 Enable	🔘 Disable		
	Client Bypass Protocol:	🔽 Inherit	🔿 Enable	🔿 Disable		
	FQDN of This Device:	FQDN				
	MTU:	🔲 Inherit	1000			
	Keepalive Messages:	🔽 Inherit	Disable	Interval:	seconds	
	Optional Client Modules to Download:	🔲 Inherit	dart,nvm			+
	Always-On VPN:	🔽 Inherit	AnyCon	nect DART	alar.	
	Client Profiles to Download:	🔽 Inherit	AnyCon	nect Network	ner Visibility	
		Add	AnyConi AnyConi	nect SBL nect Posture		
		Profile Nan	AnyCon AnyCon	nect Web Sec nect Network	urity Access Manager	
			AnyCon	nect ISE Post	re	
						DK Cancel
		L				
nd:	S Next	Previous				

Configuratie van Web-Plaatsing op Cisco ISE

Om Cisco ISE voor AnyConnect Web-Deployment te configureren voert u deze stappen uit:

1. In Cisco ISE GUI, navigeer naar **Beleid > Elementen van het Beleid > Resultaten**.

2. **Clientprovisioning** uitvouwen om **bronnen** weer te geven en **bronnen** te selecteren. Afbeelding toevoegen:

Stap 1. Selecteer Add > Agent Resources en uploaden het Any Connect pakketbestand.

the dentity Services Engine Home → Operations		istration + Work Centers			0	0	0	2	•
Policy Sets Profiling Posture Client Provisioning Policy Ele	ments								
Dictionaries Conditions Results									
Apent Resources From Local D	sk > Agent Resources From Local Disk								
Authentication Agent Resources From	Local Disk								
Authorization									
Profiling Category	Cisco Provided Packages	Ţ. Ø							
> Posture	Browse anyconnect-win-4.2.020)75-k9.pkg							
Client Provisioning									
Resources	▼ AnyConnect Uploaded Resource	es							
	Name	Туре	Version	Description					
	AnyConnectDesktopWindows 4.2.207	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clien					
Submit									

Stap 2. Bevestig de hash van de verpakking in de pop-up.

Het bestand-hash kan worden geverifieerd via de downloadpagina van Cisco.com of met een gereedschap van derden.

Deze stap kan worden herhaald om meerdere AnyConnect-afbeeldingen toe te voegen. (voor Mac OSX en Linux OS)

Please confirm this package's hash matches : SHA-1: bbce54f3fdda9a0c9d15b9331a79620e42a96b77 SHA-256: af8751ba5dedb48ca4106a71dbbdf00ccc825e4007f6180259c44e59570d9d8a
Confirm

NVM-profiel toevoegen:

Stap 1. Selecteer Add > Agent Resources en uploadt het NVM-clientprofiel.

dentity Services Engine	Home	icy → Guest Access → Ac	ministration		0	Q,	0 <u>1</u>	ø
Policy Sets Profiling Posture Cli	ent Provisioning Policy Elements							
Dictionaries Conditions Results	3							
0	Agent Resources From Local Disk > J	Agent Resources From Local Disk						
Authentication	Agent Resources From Loc	al Disk						
Authorization								
Profiling	Category	Customer Created Packages	• •					
Posture	Туре	AnyConnect Profile	Ť					
✓ Client Provisioning	* Name	AnyConnect Network Visibility						
Resources								
	Description							
		Browse NVM_serviceProfile	.xml					
	Submit Cancel							

Geef configuratie bestand toe:

Stap 1. Klik op Add en kies AnyConnect Configuration

Selecteer het pakket dat in de vorige stap is geüpload.

dentity Services Engine	Home Operations Policy G	uest Access Administratio	n 🔹 Work Cen	ters			
Policy Sets Profiling Posture Client	t Provisioning Policy Elements						
Dictionaries + Conditions - Results							
9							
	Resources						
Authentication							Selected 0 Total 56
 Authorization 	A field - Do Duplicate - M Dalate					have 40	
Addionation						now All	· 0
► Profiling	Nan Agent resources from local disk		Version	Last Update	Description		
	Win Native Supplicant Profile	Nizard	1.0.0.46	2015/10/08 02:24:16	ISE 2.0 Supplicant Provisioning		
▶ Posture	Cis AnyConnect Configuration	Supplicant Profile	Not Applicable	2015/10/08 02:24:15	Pre-configured Native Supplicant		
	Mac NAC Agent or AnyConnect Posture P	rofile XSPWizard	1.0.0.36	2015/10/08 02:24:15	ISE 2.0 Supplicant Provisioning		
✓ Client Provisioning	Wet AMP Enabler Profile	ent	4.9.0.28	2015/12/16 15:25:11	NAC WebAgent (ISE 1.1.3 release)		
	MacOsXSPWizard 1.0.0.30	MacOsXSPWizard	1.0.0.30	2015/12/16 15:25:17	Supplicant Provisioning Wizard f		
Resources	WebAgent 4.9.0.24	WebAgent	4.9.0.24	2015/12/16 15:25:24	NAC WebAgent (ISE 1.1.1 or later)		
	MacOsXAgent 4.9.0.661	MacOsXAgent	4.9.0.661	2015/12/16 15:25:32	NAC Posture Agent for Mac OS		
	MACComplianceModule 3.6.10255.2	MACComplianceModule	3.6.10255.2	2015/12/16 15:25:37	MACAgent ComplianceModule v		
	MacOsXAgent 4.9.0.1006	MacOsXAgent	4.9.0.1006	2015/12/16 15:25:44	NAC Posture Agent for Mac OS		
	NACAgent 4.9.0.52	NACAgent	4.9.0.52	2015/12/16 15:25:52	NAC Windows Agent (ISE 1.1.3		
	NACAgent 4.9.0.1009	NACAgent	4.9.0.1009	2015/12/16 15:26:06	NAC Windows Agent (ISE 1.2 rel		
	NACAgent 4.9.4.3	NACAgent	4.9.4.3	2015/12/16 15:26:21	NAC Windows Agent - ISE 1.2 , I		
	AnyConnectComplianceModuleWind	AnyConnectComplianceMo	3.6.10255.2	2015/12/16 15:26:39	AnyConnect Windows Complian		
	NACAgent 4.9.5.4	NACAgent	4.9.5.4	2015/12/16 15:26:49	NAC Windows Agent - ISE 1.2 a		
	NACAgent 4.9.5.10	NACAgent	4.9.5.10	2015/12/16 15:27:05	NAC Windows Agent - ISE 1.2.1		
	NACAgent 4.9.0.42	NACAgent	4.9.0.42	2015/12/16 15:27:19	NAC Windows Agent (ISE 1.1.1		
	MacOsXSPWizard 1.0.0.21	MacOsXSPWizard	1.0.0.21	2015/12/16 15:27:29	Supplicant Provisioning Wizard f		
	WebAgent 4.9.0.1005	WebAgent	4.9.0.1005	2015/12/16 15:27:34	NAC WebAgent (ISE 1.2 release)		
	NACAgent 4.9.5.8	NACAgent	4.9.5.8	2015/12/16 15:27:43	NAC Windows Agent - ISE 1.2 a		
	NACAgent 4.9.5.7	NACAgent	4.9.5.7	2015/12/16 15:27:59	NAC Windows Agent - ISE 1.2 a		

Stap 2. Schakel NVM in de selectie van AnyConnect Module samen met het gewenste beleid.

dentity Services Engine	Home Operations Operations Guest Access Administration Work Centers	0	0	0	2	¢.
Policy Sets Profiling Posture C	ent Provisioning Policy Elements					
Dictionaries + Conditions - Result	8					
0						
Authentication	AnyConnect Configuration > New AnyConnect Configuration					
Authorization	* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0 v					
Profiling	Configuration Name: AnyConnect Configuration					
Posture	Description:					
- Client Provisioning	Compliance Module Compliance M					
Resources						
	AnyConnect Module Selection ISE Posture VPNO Network Access Manager Web Security AMP Enabler ASA Posture Network Visibility Start Before Logon. Diagnostic and Reporting Too					

In dit gedeelte kunnen we AnyConnect-clientmodules, profielen, customization/taalpakketten en de Opswat-pakketten inschakelen.

Raadpleeg voor gedetailleerde informatie over de configuratie van webimplementatie op Cisco ISE:

Web-implementering van AnyConnect

Trusted Network Detectie

AnyConnect NVM verstuurt alleen stroominformatie als deze op een betrouwbaar netwerk is geïnstalleerd. Het gebruikt de TND-functie van AnyConnect-client om te weten of het eindpunt in een vertrouwd netwerk zit of niet.

Trusted Network Detectie is ingesteld in AnyConnect Client Profile (XML) dat voor VPN wordt gebruikt, ongeacht of de VPN-component in de omgeving is gebruikt of niet. TND is ingeschakeld door de sectie Automatisch VPN-beleid in het profiel te configureren. minimaal moet één Trusted DNS-domein of Trusted DNS-server worden ingevuld. De acties van AnyConnect wanneer de client heeft bepaald dat deze op een betrouwbaar netwerk is uitgevoerd, kunnen worden ingesteld op **DoNiets** Mode met behulp van de pull-down voor het Trusted en Unvertrouwde Network Policy.

XML Profile (excerpt)	ASDM PROFILE EDI	TOR (excerpt)
<automaticvpnpolicy>true <trusteddnsdomains>demo.local</trusteddnsdomains> <trusteddnsservers>18.1.100.l0 <trustednetworkpolicy>DoNothing</trustednetworkpolicy> <untrustednetworkpolicy>DoNothing</untrustednetworkpolicy> <alwayson>false </alwayson></trusteddnsservers></automaticvpnpolicy>	Performance Development Directed (%) P Automatic VM Policy Trutated VM Policy Untrusted Network Policy Trusted DNS Domans Trusted DNS Servers Note: adding al DNS servers in use is recommend	Dollating x Dollating x (198.19.10.1 (198.19.10.1) ed with Trusted Network Detection

S Cisco AnyCo	nnect Secure Mobility Client			x
	VPN: On a trusted network. SUA-Forum	•	Connect	
۞ ① ۞				alialia cisco

Raadpleeg voor meer informatie over de TND-configuratie: <u>Trusted Network Detectie configureren</u>

implementeren

Deployment Any Connect NVM-oplossing omvat de volgende stappen:

- 1. Configureer de NVM met AnyConnect op Cisco ASA/ISE.
- 2. Stel IPFIX Collector component (NVM Collector op Linux in Packaged in the TA Add-On) in.
- 3. Stel Splunk in met Cisco NVM App en TA Add-On.

Stap 1. Configureer de NVM via Cisco ASA/ISE

Deze stap is in detail behandeld in de sectie Configure.

Als NVM eenmaal is ingesteld op Cisco ISE/ASA, kan deze worden geautomatiseerd naar clientendpoints.

Stap 2. Stel IPFIX Collector Component in (AnyConnect NVM Collector)

De Collector Component is verantwoordelijk voor het verzamelen en vertalen van alle IPFIXgegevens van de endpoints en het doorsturen naar de <u>Splunk Add-On</u>. De NVM collector draait op 64-bits Linux. De configuratiescripts van CentOS, Ubuntu en Docker zijn opgenomen. De installatie scripts en configuratiebestanden van CentOS kunnen ook in Fedora en Redhat distributions worden gebruikt.

In een typische gedistribueerde plaatsing van Splunk Enterprise zou de verzamelaar moeten worden uitgevoerd op of een standalone 64-bits Linux-systeem of <u>Splunk Forwarder-</u>knooppunt dat op 64-bits Linux wordt gebruikt. Het kan ook op een standalone server zonder splunkcomponenten worden geïnstalleerd.

Opmerking: De oplossing kan ook worden uitgevoerd op één enkel 64-bits Linux-systeem dat de NVM-verzamelaar en Splunk Enterprise-componenten bevat voor gebruik in een kleine implementatie of voor demonstratiedoeleinden. all-in-one is het makkelijkst voor tot

Hoe installeert u de Collector?

- Kopieer de adapter.zipfile, bevindt zich in de /opt/splunk/etc/apps/\$APP_DIR\$/appserver/addon/ (meegeleverd met de TA Add-On)-map voor het systeem waarop u de map wilt installeren.
- 2. Extraceer de bestanden (unzip acnvmCollector.zip)

Het wordt aanbevolen het **\$PLATFORM\$_README-**bestand in de bundel.**zip** te lezen voordat het **install.sh** script uitvoert. Het **\$PLATFORM\$_README**-bestand bevat informatie over de relevante configuratie-instellingen die moeten worden geverifieerd en aangepast (indien nodig) voordat het **install.sh** script wordt uitgevoerd. U moet ten minste het adres van de Splunk-instantie configureren waarnaar u gegevens doorstuurt. Wanneer u het systeem niet correct instell, kan dit ertoe leiden dat de verzamelaar niet correct werkt.

Opmerking: Zorg ervoor dat de netwerk- en host-firewalls correct zijn geconfigureerd om het UDP-verkeer voor de bron- en doeladressen en -poorten toe te staan. Het IPFIX (flow) verkeer dat van de om het even welke klanten aan de verzamelaar en de uitgaande UDP gegevens aan Splunk (hier) komt.

Een enkele NVM-verzamelaar kan een minimum van 5000 stromen per seconde verwerken op een goed gesorteerd systeem. Of tot 35-40.000 eindpunten. De verzamelaar moet worden geconfigureerd en actief voordat de Splunk NVM en TA-Add op App kunnen worden gebruikt.

De standaardinstelling is dat de verzamelaar stromen ontvangt van AnyConnect NVM endpoints op UDP-poort 2055.

Daarnaast produceert de verzamelaar drie gegevensfeeds voor Splunk, Per Flow Data, Endpoint Identity Data en Endpoint Interface Data op UDP-poorten 20519, 20520 en 20521.

De poorten voor ontvangen en gegevensinvoer kunnen worden gewijzigd door het **acnvm.conf**bestand te wijzigen en de verzamelaarsinstantie te herstarten. Zorg ervoor dat elke host/netwerk firewall tussen endpoints en de verzamelaar of tussen de verzamelaar en het Splunk-systeem(s) open is voor de geconfigureerde UDP-poorten en -adressen. Zorg er ook voor dat de configuratie van AnyConnect NVM overeenkomt met de configuratie van uw verzamelaar.

Nadat alle onderdelen zijn geïnstalleerd en uitgevoerd, raadpleegt u het gedeelte Help-bestanden vanuit de Splunk-toepassing voor meer informatie over de vooraf ingestelde rapporten, het gegevensmodel en de informatie-elementen die door de oplossing zijn gemaakt.

U kunt één van uw AnyConnect-eindpunten opnieuw opstarten en valideren dat gegevens naar de oplossing worden verzonden. Start een vaste gegevensstroom met behulp van YouTube.

De informatie moet in het configuratiebestand worden geconfigureerd - acnvm.conf

- syslog_server_ip (expediteur of splunk instantie) kan naar 127.0.0.1 (gebruik LOCALHOST niet) wijzen als deze op hetzelfde doosje staat
- Het standaard poort voor de verzamelaar (inkomende IPFIX-gegevens) is niet geschikt.

OPMERKING: netflow_Collector_ip wordt weggelaten van het configuratiebestand (het gebruikt de standaard openbare interface), het zou slechts moeten worden veranderd om met een specifiek lokaal IP te omzeilen

Per Flow Data-poort, Endpoint Identity Data-poort, Endpoint Interface Data en Collector Port zijn vooraf ingesteld op standaardinstellingen in het configuratiebestand. Zorg ervoor dat deze waarden worden gewijzigd indien niet-standaard poorten worden gebruikt.

Deze informatie wordt toegevoegd in het configuratiebestand - /opt/acnvm.conf

Ondersteuning van DTLS

(zie NVM DTLS-informatie voor meer informatie)

Dit gebeurt in het doosje waarin de verzamelaar wordt getoond.

- Maak folder /opt/acnvm/certs.
- Om het certificaat toe te passen op de verzamelaar, slaat u het op met de toets in de directory opt/acnvm/certs
- wijzig de eigenaar en de groep van de map in acnvm:acnvm met deze opdracht: sudo chown -R acnvm:acnvm certs/:
- Dit gedeelte voor acnvm.conf moet worden geconfigureerd met de cert en de toets
- Nadat de configuratie en cert zijn geplaatst, start de verzamelaar sudo systemctl start acnvm.service
- Controleer de status van verzamelaar sudo systemc status acnvm.service

```
{ "security" :{ "dtls_enabled": true, "server_certificate":"/opt/acnvm/certs/public.cer",
"server_pkey":"/opt/acnvm/certs/private.key" },
```

Hier is de rest op de configuratie.

"syslog_server_ip" : "192.0.2.113", "syslog_flowdata_server_port" : 20519, "syslog_sysdata_server_port" : 20520, "syslog_intdata_server_port" : 20521, "netflow_collector_port" : 2055, "correlate_data": false } 3. het install.sh script uitvoeren met superuser privileges (zoals ./install.sh)

Opmerking: De account heeft aangepaste rechten of wortel nodig om de install.sh en de toegangsrechten voor de ACM Service Account te kunnen uitvoeren.

Raadpleeg voor meer informatie https://splunkbase.splunk.com/app/2992/#/details

Stap 3. Stel Splunk in met Cisco NVM App (CESA Dashboard) en TA Add-On voor Splunk.

Cisco AnyConnect NVM App voor Splunk is beschikbaar op de Splunkbasis. Deze app helpt met vooraf gedefinieerde rapporten en dashboards om IPFIX (nvzFlow)-gegevens te gebruiken van endpoints in bruikbare rapporten en correleert gebruiker- en endpointgedrag.

Opmerking: Voor cloudimplementaties worden beide apps geïnstalleerd in de cloudinstantie.

Alleen de technische bijstand is op het gebouw geïnstalleerd (met de expediteur). De verzamelaar wordt op het gebouw met de expediteur of op een afzonderlijk linux/docker vakje geïnstalleerd.

Voor een aanmelding kunt u alleen alle onderdelen en apps in één vak installeren (of afzonderlijk) zie diagrammen

Download deze bestanden:

- Cisco NVM App voor Splunk op Splunkbase: https://splunkbase.splunk.com/app/2992/
- Cisco NVM Add-on voor Splunk op Splunkbase: https://splunkbase.splunk.com/app/4221/

Installeren

Stap 1. Navigeer naar **Splunk > Apps** en klik op het gereedschap en installeer het bestand **tar.gz** dat u hebt gedownload van de Splunkbasis of zoekopdracht in het Apps-gedeelte.



Stap 2. Daarna moet u de **Add-On** installeren met hetzelfde proces. Controleer of beide geïnstalleerd zijn door de pagina **Splunk Apps** te bekijken:

splunk>enterprise Apps -						🚯 Admir
Apps						
cisco nvm Q						
Name 🕈	Folder name 🕈	Version \$	Update checking \$	Visible \$	Sharing \$	Status 🕈
Cisco NVM Dashboard	CiscoNVM	3.1.0	Yes	Yes	App Permissions	Enabled Disable
Cisco NVM Add-on for Splunk	TA-Cisco-NVM	3.0.9	Yes	No	App Permissions	Enabled Disable
<						

De standaardconfiguratie ontvangt drie gegevensfeeds voor Splunk, Per Flow Data, Endpoint Identity Data en Endpoint Interface Data, respectievelijk op UDP-poorten 20519, 20520 en 20521 (zie Stap 2)

De add-on zet deze dan in kaart aan Splunk source **Cisco:nvm:stroomgegevens**, **Cisco:nvm:sysgegevens** en **Cisco:nvm:ifgegevens**.

UDP-ingangen inschakelen met behulp van Splunk Management UI

Opmerking: Dit kunt u ook doen met een input.conf-bestand. Dit wordt uitgelegd in de Cisco NVM Dashboard-app in de Help-functie

U hoeft de software van Splunk niet opnieuw te starten.

Navigeer naar Splunk > Instellingen > Data Input > UDP zoals in de afbeelding.

1. Klik op New Local UDP > Voer poort in # ontbrekend > Klik op Volgende > selecteer corresponderend brontype > Klik **op Review** > Klik op Inzenden

2. Doe dit met de andere 2 poorten (probeer de kloon te gebruiken)

	Add Data	Select Source	Input Settings	Review	-O Done	< Back	Subm
		Select Stores	input dettings		0.0116		
Review							
input Type	UDP Port						
Port Number	20519						
Source name override	N/A						
Restrict to Host	N/A						
Source Type	cisco:nvm:flowdat	ta					
App Context	search						
Host	(IP address of the	remote server)					
Index	riofault						

splunk> R Apps V		
UDP Data inputs » UDP		
New		
Showing 1-3 of 3 items		
UDP port ÷	Source type ¢	Status ‡

ODP port =	Source type ÷	status ÷
20519	cisco:nvm:flowdata	Enabled
20520	cisco:nvm:sysdata	Enabled
20521	cisco:nvm:ifdata	Enabled

Verifiëren

AnyConnect NVM-installatie valideren

Na een succesvolle installatie moet de netwerkzichtbaarheidsmodule worden opgenomen in **geïnstalleerde modules,** in het gedeelte **Informatie** van de client voor Any Secure Mobility.



Controleer ook of de nvm-service op het eindpunt wordt uitgevoerd en het profiel in de vereiste map staat.

Valideren van Collector status als actief

Zorg ervoor dat de status van de verzamelaar actief is. Dit waarborgt dat de verzamelaar te allen

tijde IPFIX/flow uit de eindpunten ontvangt. Als deze niet actief is, zorg er dan voor dat de cnvm account rechten voor het bestand het uitvoeren toestaan: **/opt/acnvm/bin/acnvmcollector**

root@ubuntu-splunkcollector:~\$ /etc/init.d/acnvmcollectord status
* acnvmcollector is running
root@ubuntu-splunkcollector:~\$
<pre>[splunk@splunk-virtual-machine addon]\$ systemctl status acnvm.service • acnvm.service - AC NVM Service Loaded: loaded (/usr/lib/system/system/acnvm.service; enabled; vendor preset: disabled) Active: active (running) since Fri 2020-06-19 13:48:08 EDT; 25s ago Main PID: 41165 (acnvmcollector) Tasks: 13 (limit: 49772) Memory: 1.8M Computer active (running) service</pre>
<pre>condp. /system.stree/activm.conf -1 /opt/activm/conf/activm.conf -1 /opt/activm.conf -1 /opt/</pre>

Splunk valideren - AnyConnect NVM CESA Dashboard

Zorg ervoor dat Splunk en zijn relevante services actief zijn. Raadpleeg hun website voor documentatie over het oplossen van problemen met Splunk.

Niet de dashboards voor CESA zullen niet worden bijgewerkt tot 5 minuten nadat de eerste gegevens zijn ontvangen vanwege een automatiseringsscript. Start een handmatige zoekopdracht om direct te valideren:

Klik vanaf het hoofddashboard op "Zoeken en rapporteren". Stel in het volgende scherm het juiste bereik in om de gewenste gegevens op te geven en waar er op staat: "Typ hier zoekopdracht...". Voer "sourcetype="cisco:nvm:flow data" in

sourcetype="cisco:nvm:f	flowdata"											Last 19	5 minutes	
1,608 events (9/1/20 3:29	252.000 PM to	9/1/20	3:44:52.00D PM)	No Event Sampling *			Job 🔻	П	۰.	ð	ð.	Ŧ	♥ Sma	rt Mode 🔻
Events (1,608) Patterns	s Statistics	VI	sualization											
Format Timeline • -	Zoom Out	+ Zoo	m to Selection	× Deselect									1 minu	te per column
		List	💌 🖌 Format	20 Per Page *		< Prev	1	2 3	4	5	6	7	8	Next >
< Hide Fields	Ξ All Fiαlds	i	Time	Event										
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS a action 1		>	9/1/20 3:44:08.000 PM	Sep 1 15:44:88 138.18.133.42 Se p="443" fss="153839066" fst="Tu D3A2122688371A188FAF526" liuid= exe" ph="C5095E1AA5A65C228BA81A2 xe" ph="C5095EFF326A8C4077A62340 known" iid="162" ml=""" ml="" host = 19818133.42 source = sys	p 1 15:44:08 splunk-vi te Sep 1 15:37:46 2028" "''' liuat-"0' pa="NT A FE657FDA1F09C2ACBC4589E '' liuidp="unknown" slog sourcetype clscc	rtual-machine fes="159898944 UTHORITY\SYSTEM 952C48534825429 95F0EC488919C38	pr="6" s 7" fet=" " paa="M 174" ppa 489" ibc	а="198 Tue Sej T AUTH ="NT AJ ="1092)	.19.18 D 1 1 DRITY" UTHORJ Ə" obc	1.36" 5:44: ' pap= TY\SY :="404	sp="4 07 20 "SYST STEM" 8" ds	9692" o 20" udi EM" pua ppuat= ="dcloo	da="198. dd="6861 dt="2" p "2" ppn d.cisco	19.10.100° d 6875A273996E n="vpnagent. ="services.e .com" dh="Un

Controleer het Splunk Dashboard om ervoor te zorgen dat Ga naar Splunk, klik op **Cisco NVM Dashboard**, klik op **Apparaatactiviteit door volume en Flow Count** als u de huidige instellingen wilt behouden en klik op **Inzenden**. Het geeft gegevens in de illustratie weer.

PacketFlow

- 1. IPFIX-pakketten worden gegenereerd op client-endpoints door AnyConnect NVM-module.
- 2. De client-eindpunten sturen IPFIX-pakketten naar het IP-adres van de verzamelaar.

3. De verzamelaar verzamelt de informatie en stuurt deze naar Splunk.

4. Verzamelaar stuurt op drie verschillende stromen verkeer naar Splunk: Per Flow data, endpointgegevens en interfacegegevens.

Al het verkeer is UDP dat is gebaseerd op de afwezigheid van ontvangstbevestiging.

Standaardpoort voor verkeer:

IPFIX-gegevens 2055

Per Flow Data 2019

Endpoint Data 20520

Interfacegegevens 20521

NVM-module slaat IPFIX-gegevens op en stuurt deze naar een verzamelaar wanneer deze zich in Trusted Network bevindt. Dit kan zijn wanneer de laptop is aangesloten op het bedrijfsnetwerk (on-prem) of wanneer hij via VPN is verbonden.

U kunt valideren dat de verzamelaar pakketten ontvangt van de NVM-module door een pakketvastlegging op specifieke UDP-poorten uit te voeren, zoals in uw configuratie wordt aangegeven om te controleren of de pakketten worden ontvangen. Dit gebeurt via het Splunksysteem linux OS.

Flow-sjablonen

De IPFIX-stroomsjablonen worden naar de verzamelaar gestuurd aan het begin van de IPFIXcommunicatie. Deze sjablonen helpen de verzamelaar om de IPFIX-gegevens te begrijpen.

De verzamelaar voegt ook sjablonen toe om er zeker van te zijn dat zelfs als de klant ze niet heeft verstuurd, de gegevens kunnen worden geparseerd. Als een nieuwere versie van de client wordt vrijgegeven met protocolwijzigingen, worden de nieuwe sjablonen gebruikt die door de client worden verstuurd.

Een sjabloon wordt onder deze voorwaarden verzonden:

- 1. Er is een verandering in het NVM-clientprofiel.
- 2. Er is een evenement voor netwerkverandering.
- 3. De spoeddienst is opnieuw gestart.
- 4. Het eindpunt wordt herstart/herstart.
- 5. Periodiek (standaard=24 uur) zoals ingesteld in het NVM Profile.

In zeldzame gevallen is er mogelijk geen sjabloon gevonden. Dit kan eenvoudig worden verholpen door een van de eindpunten opnieuw te starten.

De kwestie kan worden geïdentificeerd door het observeren van **geen sjabloon** die **is gevonden** in een pakketvastlegging op het eindpunt of **geen sjablonen voor stromen die zijn ingesteld** in de collector logs.

Problemen oplossen

Dit zijn de basisstappen voor probleemoplossing:

- 1. Zorg voor netwerkconnectiviteit tussen client-eindpunt en verzamelaar.
- 2. Zorg voor netwerkconnectiviteit tussen verzamelaar en splunk.
- 3. Zorg ervoor dat NVM op de juiste manier op het clienteindpunt is geïnstalleerd.
- 4. Pas opnames op het eindpunt toe om te zien of het IPFIX verkeer wordt gegenereerd.
- 5. Toepassen opnames op een verzamelaar om te zien of het IPFIX verkeer ontvangt en of het verkeer naar Splunk doorgeeft.
- 6. Toepassen opnames op Splunk om te zien of het verkeer ontvangt.
- 7. Voor DTLS alle klanten die vertrouwen op het verzamelaarscertificaatNVM-profiel is beveiligdverzamelaar is ingesteld voor certs

IPFIX-verkeer zoals in Wireshark gezien:

Opmerking: Als u DTLS tussen de client en de verzamelaar gebruikt, moet u een filter op DTLS-verkeer filteren

Ap	ply a display filter <ctrl-></ctrl->						Expression +	
No.	Tim Source	Destination	Protocol	Length	Info			
F	1 0 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	2 0 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	3 0 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	4 0 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	5 0 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	6 2 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	7 0 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]	-	
	8 1 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	9 2 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	10 2 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	11 2 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	12 0 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	13 0 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		
	14 2 192.168.100.1	10.76.76.161	CFLOW	269	IPFIX	flow (227 bytes) Obs-Domain-ID= 127 [Data:258]		1

AnyConnect-client (NVM-module)

AnyConnect NVM - niet rapporteren aan de Collector - CFLOW-datapakketten blijven geen eindpunt achter

Groeit het NVM database bestand onder C:\%ProgramData%\Cisco\Cisco Anyconnect Secure Mobility Client? Als het blijft groeien betekent dit dat de logboeken niet van de klant worden verstuurd.Als je onder de NVM-map kijkt, zie je dat de sql-database groeit, dan is de nvm.db niet gedocumenteerd, maar we praten uitgebreid over hoe we caching in de <u>NVM-gids</u> en de controles rond caching in <u>de NVM-gids</u>. Als je dat ziet, stuurt het de gegevens niet naar de verzamelaar.

07/02/2020	06:00 PM	<dir></dir>	
07/02/2020	06:00 PM	(DIR)	
07/02/2020	05:54 PM	514	KConfig.dat
07/02/2020	06:00 PM	20,480	NVM.db
06/12/2020	08:36 PM	937	NVM_ServiceProfile.xml
07/02/2020	05:00 PM	2	PersistedData.dat
	4 File(s) 21,933	3 bytes
	2 Dir(s)	6,818,320,384	bytes free

Trusted Network Detection (TND)

Start AnyConnect UI en zorg ervoor dat dit op een betrouwbaar netwerk gebeurt. NVM is

afhankelijk van TND voor het detecteren van het eindpunt in een betrouwbaar netwerk. Als de TND-configuratie niet correct is, levert dit problemen op met NVM. NVM heeft zijn eigen TND-configuratie, die werkt op de TLS-certificaatvingerafdruk van de geconfigureerde server. Dit kan worden ingesteld in de NVM Profile Editor.

Als NVM TND niet is geconfigureerd, is NVM afhankelijk van de TND-configuratie van de VPNmodule. VPN's TND werkt op basis van informatie die via DHCP wordt ontvangen: domeinnaam en DNS-server. Als de DNS-server en/of de domeinnaam overeenkomen met de ingestelde waarden, wordt het netwerk als betrouwbaar beschouwd. VPN ondersteunt ook TLS op certificaat gebaseerde TND-detectie.

- Zorg ervoor dat de Trusted Network Detectie-configuratie juist is. NVM exporteert alleen wanneer dit op een betrouwbaar netwerk gebeurt, d.w.z. een ongeldige TND-configuratie (bijvoorbeeld: als u 3 DNS-servers hebt, hebt u 3 gedefinieerd) nodig.
- Verwijder het vertrouwde domein van de TND VPN-configuratie
- Netwerkkwesties: gesplitste tunneling (het IP-adres van de verzamelaar maakt geen deel uit van de gesplitste tunnel die wordt vertrouwd, zodat de gegevens worden verzonden naar de openbare interface). Zorg ervoor dat de IP van de verzamelaar altijd in de splitsingen zit, ook voor VPN.
- Zorg ervoor dat de Collector is ingesteld om deze op het huidige netwerk te verzamelen (vertrouwde/onvertrouwde).
- Zorg ervoor dat de mappen VPN.xml en NVM_ServiceProfile.xml in de juiste mappen staan en opnieuw starten
- Start-stop alle aansluitingsservices
- Staak het netwerk dat op de binnenkant is aangesloten en dat een verbinding met de DNS server heeft.

PacketCapture:



AnyConnect diagnostiek en rapportage-tools (DART)

Om een oplossing te vinden doet AnyConnect DART uitvoeren op de NVM-onderdelen.

- Alle logbestanden die nodig zijn voor NVM worden door DART verwerkt, worden opgeslagen, geconfigureren, enzovoort.
- Windows logs Evenementen zijn niet op één locatie, er is een apart blad in de eventviewer voor NVM onder AnyConnect.
- macOS/linux filterbestanden per medium

Collector (op Linux/Docker machine - all-in-one of standalone)

acnvmCollector is niet geïnstalleerd :

Terwijl u verzamelaar installeert en het script installeert

Sudo ./install_ubuntu.sh

Ik krijg een fout in de var/log/syslog. "Acnvm.conf-fout: regel nummer 17 : verwacht belangrijke string" dit was omdat er een komma was waar je niet zou moeten zijn, misschien nog een extra

acnvmCollector kan niet starten :

Dit was een probleem op Ubuntu (maar mogelijk voor alle linux). Ik merkte op dat de code niet in het collectorbestand is uitgevoerd: **/opt/acnvm/bin/acnvmcollector**.

De actieve gebruiker en de groep hadden geen eXecute voor de adapter



Collector logs

Hoe kan ik verificaties van de verzamelaar verkrijgen?

./nvmcollector -v Waar kan ik het debug instellen?

U kunt het logniveau in ACMNVMLOG.conf instellen - het gedeelte van de configuratie dat naar het opstartbeeld van de computer wordt verzonden. Start na een verandering de verzamelaar opnieuw op.

log4cplus.rootLogger=DEBUG, STDOUT, NVMFileAppender < dit is te vinden in **ACNVMLOG**.conf-bestand

```
Jan 20 12:48:54 csaxena-ubuntu-splunkcollector NVMCollector: no templates
for flowset 258 for 10.150.176.167 yet
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector:
HandleReceivedIPFIX: exporter=10.150.176.167 bytes_recvd=234 totlength=234
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector:
=============> flowsetid=258 flowsetlen=218
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector: no templates
for flowset 258 for 10.150.176.167 yet
```

DTLS-kwesties:

- DTLS niet ingesteld (middelen zijn niet gezien in het acnvm.conf-bestand)
- De servertoets is ongeldig (dit was een toetsencombinatie met het wachtwoord dat niet wordt

Splunk Console (NVM Dashboard) geeft geen gegevens weer

AnyConnect-client

- Gegevens genereren met behulp van YouTube en misschien browsen naar een paar website
- Kan een client informatie via UDP 2055 naar de verzamelserver sturen (zijn er daartussen firewalls?) probeert telnet van clientmachine naar verzamelmachine
- Draai draadloos shark om er zeker van te zijn dat de client verkeer (2055 cflow) gegevens naar de verzamelaar stuurt

Verzamelbak

- Waarderen van het ontvangen van AnyConnect NVM-verkeer Voer een bom uit (en zorg ervoor dat u pakketten van client tot server op 25001 tot 2055 ziet) Sudo tcPDump -I anyc100-nn host 10.1.10.7 (dit betekent dat eerst 100 pakketten afkomstig zijn van IPclienthost)<u>Hoe wordt TCPDUMP op tellers gebruikt</u>
- Zorg ervoor dat de NVM-verzamelaar van anyconnect actief is (zie bovenaan informatie met behulp van het systeem)
- Controleer cnvm.conf op de opmaak, ontbrekende quotes, komma's enz
- Splunk UI TA zijn de UDP-gegevensinvoer en de productie van brongegevens die zijn ingesteld op de Splunk GUI of via Input.conf Start opnieuw op onder UI > Instellingen > servercontroles

Vaak gestelde vragen (veelgestelde vragen)

1. Hoe kunt u gegevens van een willekeurige NVM naar meerdere bestemmingen sturen?

Dit wordt gebruikt voor een hoge beschikbaarheid of voor het verzenden naar Splunk en Stealthwatch.

Zie voor meer informatie http://cs.co/cesa-pov

2. Waar slaat u het certificaatmodel op voor AnyConnect NVM DTLS?

Dit zou voor laboratoriumtesten zijn waar geen bekende cert geïnstalleerd is op de verzamelaar.

Windows

Installeer het certificaat van de verzamelaar in de Windows Vertrouwde certificaten

Mac OSX

Voor het installeren van het wortelcertificaat is het proces standaard en duidelijk gedefinieerd voor macOS dat via een sleutelketen verloopt, kunnen we Trefkettinggereedschap gebruiken om te

importeren en toe te voegen zoals u wilt.

• Linux - verschillend voor elke distro (Ubuntu en RHEL).

RHEL Root CA-IMPORTASTAPPEN:

- 1. Kopieer de cabine naar enz/pki/ca-trust/bron/ankers
- 2. sudo update-ca trust
- 3. Ten slotte sudo update-ca-trust extract

Ubuntu Root CA IMPORT STAPS :

1. K-bestand converteren naar .crt-bestand. openssl x509 - stelt PEM-in RootCA.cer-out rootCa.crt

2. Kopieer het .crt-bestand naar /usr/local/share/ca-certificaten

3. Start de opdracht sudo update-ca-certificaten

XML-bestandsnamen

Wanneer u de lokale profieleditor gebruikt. De XML-profielnaam van de kern VPN-module doet er niet toe. "Sla het profiel op als NVM_ServiceProfile.xml. U moet het profiel met deze exacte naam opslaan, anders kan NVM gegevens niet verzamelen en verzenden."

Collector (anyconnect NVM)

https://splunkbase.splunk.com/app/2992/#/details

- Kan een folder onder wortel worden gemaakt en daarna het eigendom aan een andere rekening worden verstrekt? U kunt eerst **een** NVM maken/**opteren/nvm maken** zolang het installatiescript toestemming heeft om bestanden te kopiëren
- Bestandsrechten install.sh moet toegangsrechten om als root te implementeren
- dienstrekeningen: Waarom gebruiker add -r, en waarom s/bin/vals omdat het een niet interactieve account zonder adresdirectory isHet is geen vereiste dat een adresboekje en de standaardpraktijk van de dienstrekening geen "clean"-account hebbenAlle gebruikers hebben uid/gids of zij al dan niet een huisfolder hebben.
- Verzamelaar OS stelt CentOS, Ubuntu, Redhat kunnen gebruiken CentOS script.
- Installeer het script kan indien nodig worden aangepast. Moet worden uitgevoerd als root of met SUDO rechts omdat het een nieuwe gebruiker creëert die acnvm heet en alles in een opt/acnvm directory plaatst. Algemene opmerking: U kunt ook uw eigen script maken om te doen wat u volgens uw vereisten moet doen. Dit script kan een andere gebruiker gebruiken die al op het systeem actief is, maar deze gebruiker heeft SUDO-rechten nodig om de installatie te kunnen uitvoeren.
- De collector versie werkt met -v flag ./opt/acnvm/bin/acnvmcollector-v

Aanbevolen release

Cisco raadt altijd de nieuwste softwareversie van AnyConnect aan op het moment van gebruik of update. Wanneer u de AnyConnect-versie kiest, gebruikt u de nieuwste 4.9.x-client of hoger. Dit levert de meest recente verbeteringen met betrekking tot NVM.

AnyConnect 4.9.0086 nieuwe functies

Dit is een belangrijke release die deze functies bevat en updates ondersteunt, en die de tekortkomingen oplost die in <u>AnyConnect 4.9.0086</u> worden beschreven

• NVM-uitbreiding om stroom- en endpointgegevens te verrijken, inclusief nieuwe NVM Collector, gecoördineerd met Splunk-app 3.x en een tijdstempel voor stroominformatie.

Gerelateerde informatie

- <u>Cisco Endpoint Security Analytics op Splunk (Quick Start Guide)</u>
- <u>Cisco AnyConnect Network Visibility and (NVM) app voor Splunk</u>
- Splunk Documentatie over Splunk Collector Setup en het installeren van collector scripts
- <u>Cisco AnyConnect Secure Mobility Client-beheergids</u>
- <u>Releaseopmerkingen van AnyConnect 4.x</u>
- <u>Technische ondersteuning en documentatie Cisco Systems</u>