cEdge 라우터에 UTD 보안 가상 이미지 설치

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 Cisco IOS XE SDWAN 소프트웨어를 실행하는 라우터(16.x) Cisco IOS XE Software를 실행하는 라우터(17.x) 구성 1단계. 가상 이미지 업로드 2단계. 디바이스 템플릿에 보안 정책 및 컨테이너 프로필 하위 템플릿 추가 3단계. 보안 정책 및 컨테이너 프로필로 디바이스 템플릿 업데이트 또는 첨부 다음을 확인<u>합니다.</u> 일반적인 문제 문제 1. 오류: 다음 장치에 컨테이너 소프트웨어 서비스가 없습니다. 문제점 2. 사용 가능한 메모리가 부족합니다. 문제 3. 잘못된 참조 문제 4. UTD가 설치되어 있고 활성화되어 있지만 활성화되지 않았습니다. 관련 정보

소개

이 문서에서는 Cisco IOS XE SD-WAN 디바이스에서 보안 기능을 활성화하기 위해 UTD(Unified Threat Defense) 보안 가상 이미지를 설치하는 방법에 대해 설명합니다.

사전 요구 사항

- 이러한 기능을 사용하기 전에 관련 보안 가상 이미지를 vManage 리포지토리에 업로드하십시 오.
- cEdge 라우터는 템플릿이 미리 연결된 vmanage 모드여야 합니다.
- IPS(Intrusion Prevention System), IDS(Intrusion Detection System), URL 필터링(URL-F) 또는 AMP(Advanced Malware Protection) 필터링을 위한 보안 정책 템플릿을 생성합니다.

요구 사항

- 4000 Integrated Services Router Cisco IOS XE SD-WAN(ISR4k)
- 1000 Integrated Services Router Cisco IOS XE SD-WAN(ISR1k)
- 1000v 클라우드 서비스 라우터(CSR1kv),
- 1000v ISRv(Integrated Services Router)
- 8GB DRAM을 지원하는 cEdge 플랫폼입니다.

사용되는 구성 요소

- Cisco UTD 가상 이미지
- vManage 컨트롤러
- 컨트롤러와 제어 연결이 있는 cEdge 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco UTD 이미지는 디바이스 템플릿에 보안 정책을 설치해야 하며, cEdge 라우터의 IPS(Intrusion Prevention System), IDS(Intrusion Detection System), URL 필터링(URL-F), AMP(Advanced Malware Protection) 등의 보안 기능이 활성화되어 있어야 합니다.

소프트웨어 Cisco에서 Cisco UTD Snort IP Engine <u>소프트웨어 다운로드</u>

현재 Cisco IOS XE 버전에서는 Cisco UTD 가상 이미지 지원 regex를 사용합니다. 권장 및 지원되 는 **UTD 이미지**를 검증하려면 show utd engine standard version 명령을 사용합니다.

Router01# show utd engine standard version IOS-XE Recommended UTD Version: 1.0.13_SV2.9.16.1_XE17.3 IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.3\$

참고 이미지를 다운로드할 경로는 라우터가 Cisco IOS XE SDWAN 소프트웨어(16.x) 또는 범용 Cisco IOS XE 소프트웨어(17.x)를 실행하는지에 따라 다릅니다.

Cisco IOS XE SDWAN 소프트웨어를 실행하는 라우터(16.x)

Cisco UTD Snort IPS Engine 소프트웨어를 다운로드할 수 있는 경로는 라우터/SD-WAN(Software-Defined WAN)/XE SD-WAN 라우터 및 Series Integrated Router입니다.

Downloads Home / Routers / Software-Defined WAN (SD-WAN)		
Cisco Interfaces and Modules	Cloud Connectors	Meraki vMX
Cloud and Systems Management	Cloud Edge	SD-WAN
Collaboration Endpoints	Data Center Interconnect Platforms	XE SD-WAN Routers
Conferencing	Industrial Routers and Gateways	vEdae Router
Connected Safety and Security	Mobile Internet Routers	
Contact Center	Network Functions Virtualization	
Data Center Analytics	Service Provider Core Routers	
Hyperconverged Infrastructure	Service Provider Edge Routers	
IOS and NX-OS Software	Service Provider Infrastructure Software	
Optical Networking	Small Business Routers	
Routers	Software-Defined WAN (SD-WAN)	

cEdge 라우터의 모델 유형을 선택합니다.

참고 UTD 기능에는 ASR(Series Aggregation Services Router)을 사용할 수 없습니다.



유형 라우터 모델을 선택한 후 **Cisco IOS XE SD-WAN 소프트웨어 옵션**을 선택하여 16.x 버전의 cEdge용 UTD 패키지를 가져옵니다.

Downloads Home / Routers / Software-Defined WAN (SD-WAN	/ XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN
Select a Software Type IOS XE In-Service Software Upgrade (ISSU) Matrix IOS XE SD-WAN Software IOS XE Software	

참고 cEdges 라우터용 16.x 코드의 Cisco UTD 가상 이미지를 선택하는 다운로드 경로에는 Cisco IOS XE 소프트웨어 옵션도 표시됩니다. 이는 17.x에 대해서만 cEdge의 업그레이드 코 드를 선택하는 경로이지만, 버전 17.x에 대한 UTD 가상 이미지는 없습니다. Cisco Unified Regular Cisco IOS XE 및 Cisco IOS XE SDWAN 코드는 17.x 및 최신 버전이므로 17.x용 Cisco UTD 가상 이미지를 가져오는 경로는 일반 Cisco IOS XE 코드와 동일합니다.

cEdge의 현재 버전을 선택하고 해당 버전의 UTD 패키지를 다운로드합니다.

Downloads Home / Routers / Software-	Defined WAt	N (SD-WAN) / XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN / IOS)	KE SD-WAN Software- 16	.12.5(MD)	
Q Search		ISR 4000 Series IOS XE SD-WAN	Polatod Links ar	nd Documentation	
Expand All Collapse All Suggested Release) ~	My Notifications	Release Notes for 19. Release Notes for 16.	2.4 12.5	
Latest Release	~	File Information	Release Date	Size	
16.12.5(MD) 😋 All Release	~	Cisco ISR 4200 Series IOS XE SD-WAN Software isr4200-ucmk9.16.12.5.SPA.bin Advisories 💕	29-Jan-2021	482.84 MB	±₩∎
16 Deferred Release	> ~	Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	557.83 MB	±∵≓∎
16	>	Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.12.5.SPA.bin Advisories 🗗	29-Jan-2021	621.88 MB	±₩∎
		Cisco ISR 4400v2 Series IOS XE SD-WAN Software isr4400v2-ucmk9.16.12.5.SPA.bin Advisories 🗗	29-Jan-2021	623.49 MB	±₩∎
		UTD Engine for IOS XE SD-WAN secapp-ucmk9.16.12.05.1.0.18_SV2.9.16.1_XE16.12.x86_64.tar Advisories	29-Jan-2021	52.01 MB	±₩∎

Cisco IOS XE Software를 실행하는 라우터(17.x)

Cisco IOS XE 릴리스 17.2.1r 및 최신 버전에서는 universalk9 이미지를 사용하여 Cisco IOS XE SD-WAN 및 Cisco IOS XE를 Cisco IOS XE 디바이스에 모두 구축합니다. UTD Snort IPS Engine 소프트웨어는 Routers > Branch Routers > Series Integrated Router에 있습 니다.



라우터의 모델 유형을 선택한 후 UTD Snort **IPS Engine Software를 선택합니다**.

Software Download

Downloads Home Select a Software Type IOS XE In-Service Software Upgrade (ISSU) Matrix IOS XE Patch Upgrades IOS XE ROMMON Software IOS XE SD-WAN Software IOS XE Software UTD Snort IPS Engine Software VTD Snort Subscriber Signature Package Very High Bitrate (VDSL) PHY Firmware Very High Bitrate DSL (VDSL) Firmware

라우터의 현재 버전을 선택하고 선택한 버전에 대한 UTD 패키지를 다운로드합니다.

Software Download

Downloads Home / Routers / Branch Routers / 4000 Series Integrated Services Routers / 4221 Integrated Services Router / UTD Snort IPS Engine Software- 17.7.1a									
Q Search Expand All Collapse All Latest Release	~	4221 Integrated Services Router Release 17.7.1a My Notifications	Related Links and	d Documentation locumentation -					
17.7.1a									
16.6.7a		File Information UTD Engine OVA for 17.7.1 release iosxe-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.ova	Release Date 30-Nov-2021	Size 147.72 MB					
All Release	>	UTD Engine for IOS XE secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar	30-Nov-2021	52.51 MB					
17 16	> >	Advisories 📑							

참고: 비디오 코드 대신 Cisco IOS XE Software를 실행하는 Cisco ISR1100X Series 라우터 (Cisco Nutella Routers SR1100X-4G/6G)는 x86_x64를 기반으로 합니다. ISR4K용으로 게시 된 Cisco UTD 가상 이미지가 이 라우터에서 작동합니다. 현재 Cisco IOS XE SDWAN 버전에 대해 지원되는 동일한 Cisco UTD 이미지 코드 버전을 Nutella 라우터에 설치할 수 있습니다. 권장 및 지원되는 **regex** Cisco **UTD** 이미지를 검증하려면 show utd engine standard version 명령을 사용합니다.

구성

1단계. 가상 이미지 업로드

가상 이미지가 cEdge의 현재 Cisco IOS XE SDWAN 코드와 일치하는지 확인하고 vmanage 리포지 토리에 업로드합니다.

Maintenance(유지 관리) > Software Repository(소프트웨어 저장소) > Virtual Image(가상 이미지) > Upload Virtual Image(가상 이미지 업로드) > vManage로 이동합니다.



=	Cisco vManag			•		40		
		FTWARE REPOSITORY						
	Software Images Vir	rtual Images						
\$	O Upload Virtual Imag	ge 👻 🕒 Add Custor	n VNF Package					08
3	Q		Search Options 🗸					Total Rows: 1
`	Software Version		Upload Virtual Image to vManage X	Availa				
	2.2.1	vmanage		SDAVO	_sdavc_cont	tainer_2.2.1,	_19.2.3-sd	avc.tar
<u></u>			Do not refresh the web Browser or click web Browser Back button while image is being uploaded File [Inloading (Total-1)]					
83								
_			secapp-utd.17.04.01b.1.0.9_SVZ.9.16.1_XE17.4.x86_64.tar					
			Prease wait. Server is Processing					

Cisco UTD 가상 이미지가 성공적으로 업로드되면 저장소에 있는지 다시 확인합니다.

MAINTENANCE SOFTWARE REPOSITORY				Virt	Virtual image uploaded successfully				
Software Images Virtua	al Images								
Upload Virtual Image	- Add Custo	m VNF Package							
• oprodu tintuur intege									
Q		Search	Options 🗸						
-									
Cisco vManage						▲ ¹	🔎 🚱 ia	aestrad •	
MAINTENANCE SOFTWARE REPOSITORY									
Software Images Virtual Images									
								-	
 Upload Virtual Image - O Add Custon 	n VNF Package							OE	
Q	Search Options 🐱						Tot	tal Rows: 8	
Software Version Software Location	Network Function Type	Image Type	Architecture	Version Type Name	Vendor	Available Files	Updated On		
1.0.16_SV2.9.16.1_XE17.3 vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.16	05 Nov 2021 2:39:19 PM	M	
1.0.13_SV2.9.16.1_XE17.3 vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.13	05 Nov 2021 11:31:22 A		
1.0.12_SV2.9.16.1_XE17.4 vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12	05 Nov 2021 3:51:20 PM	M ***	
1.0.12_SV2.9.13.0_XE16 vmanage	App-Hosting	Lxc	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.12	24 Jul 2020 10:50:24 AM	M	
1.0.12_SV2.9.13.0_XE16 vmanage	App-Hosting	Lice	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12	24 Jul 2020 10:50:17 AM	M	
1.0.10_SV2.9.13.0_XE17.3 vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10	16 Jan 2021 9:40:36 PM	d	
	Ann Mastina	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10	18 May 2020 10:10:22 A	A	
1.0.10_SV2.9.13.0_XE16 vmanage	Abburg								

2단계. 디바이스 템플릿에 보안 정책 및 컨테이너 프로필 하위 템플릿 추가

이전에 생성한 보안 정책을 디바이스 템플릿에 추가합니다. 보안 정책에는 디바이스 템플릿에 대한 IPS/IDS, URL-F 또는 AMP 필터링 정책이 있어야 합니다. 컨테이너 프로필을 자동으로 엽니다. 기 본 컨테이너 프로필을 사용하거나 필요한 경우 수정합니다.

Security Policy	installpartition	•
Container Profile *	Factory_Default_UTD_Template	•

3단계. 보안 정책 및 컨테이너 프로필로 디바이스 템플릿 업데이트 또는 첨부

템플릿을 업데이트하거나 cEdge 라우터에 연결합니다. 컨피그레이션 차이에서 IPS/IDS, URL-F 또 는 AMP 필터링 기능에 대한 앱 호스팅 컨피그레이션 및 UTD 엔진이 구성되었음을 확인합니다.

	258	app-hosting appid utd
	259	app-resource package-profile cloud-low
	260	app-vnic gateway0 virtualportgroup 0 guest-interface 0
	261	guest-ipaddress 192.168.1.2 netmask 255.255.255.252
	262	- 1
	263	app-vnic gatewayl virtualportgroup 1 guest-interface 1
	264	guest-ipaddress 192.0.2.2 netmask 255.255.255.252
	265	- 1 · · · · · · · · · · · · · · · · · ·
	266	start
	267	1 Contraction of the second
258	268	lldp run
259	269	nat64 translation timeout tcp 60
260	270	nat64 translation timeout udn 1
	271	utd multi-tenancy
	272	utd engine standard multi-tenancy
	273	threat-inspection profile GPC_IPS_v06_copy_copy
	274	threat detection
	275	policy security
	276	logging level warning
	277	4
	278	utd global
	279	
	280	- I
	281	policy
	282	no app-visibility
	283	no flow-visibility
	284	no implicit-acl-logging
	285	log-frequency 1000

vmanage에서 적용된 컨피그레이션에 UTD 엔진 기능**이 있음**을 발견하여 템플릿 상태가 Donescheduled로 변경되었습니다. 따라서 vmanage는 cEdge에서 UTD 보안 기능을 사용하려면 가상 이미지를 설치해야 한다고 판단합니다.

Push	Push Feature Template Configuration 🤣 Validation Success 👻								
Total Task: 1 Done - Scheduled : 1									
Q			Search Options 🗸						
>	Status		Message	Chassis Number	Device Model	Hostname	System IP	Site ID	
>	Done - Scheduled		Device needs to install some ap	CSR-FDCDD4AE-4DB9-B79B-8FF	CSR1000v	ZBFWTest	70.70.70.1	70	

템플릿이 일정 상태로 이동하면 작업 메뉴에 **진행 중인** 새 작업이 나타납니다. 새로운 작업은 Lxc **설치이며**, 이는 새 컨피그레이션을 푸시하기 전에 vmanage가 자동으로 cEdge에 가상 이미지 설치 를 시작함을 의미합니다.



LX 컨테이너가 설치되면 vManage는 UTD 기능을 사용하여 사전 예약 구성을 푸시합니다. 이전에 컨피그레이션이 예약되었기 때문에 이 작업에 대한 새 작업이 없습니다.

TASK VIEW			
Lxc Install Validation Success +			Initiated By: system From: 1.1.1.9
Total Task: 1 Success : 1			
٩	Search Options 🗸		o 🖨 Total Rows: 1
> Status	Device IP	Message	Start Time
Y Success	70.70.70.1	Done - Lxc Install	05 Nov 2021 12:06:03 PM CST
(5-M0Y-2021 18:06:03 UTC) T (5-M0Y-2021 18:06:03 UTC) S (5-M0Y-2021 18:06:04 UTC) C (5-M0Y-2021 18:06:04 UTC) C (5-M0Y-2021 18:06:09 UTC) C (5-M0Y-2021 18:06:20 UTC) C (5-M0Y-2021 18:06:20 UTC) D	otal number of Container apps to be installed: 1. Container apps to be installed arc tarted 1/1 kx countainer (app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_X8 hecking if tox is enabled on device and structure and active and the structure and the structure-x86_64_1.0.13_SV2.9.16.1_X817.3_sec onnection Instance: 4, Color: biz-internet ownloading http://l.1.9:8080/software/package/lxc/app-hosting_UTD-Snort-Feature-x8	f following: [app-hosting_UTO-Snort-Feature-x86_64-1.0.13_SV2.9.16.1 [17.3] installation ccapp-utd.17.03.03.1.0.13_SV2.9.16.1_XE17.3.x86_64.tar %6_64_1.0.13_SV2.9.16.1_XE17.3_secapp-utd.17.03.03.1.0.13_SV2.9.16.1	_XE17.3] _XE17.3.x86_64.tar?deviceId=70.70.70.1

다음을 확인합니다.

cEdge가 vManage 및 연결된 템플릿과 동기화되어 있는지 확인합니다.

Configuration(컨피그레이션) > Devices(디바이스)로 이동합니다.

CONFIGURATION DEVICES								
WAN Edge List Controllers Unclaimed WAN Edges								
[] Change Mode 👻 👤 Upload WAN Edge List 🛛 Export Bootstrap Configuration 🖾 Sync Smart Account								
Q 70.70.70.1 ×	Search Options 🗸							
Enterprise Cert Expiration Date	Subject SUDI serial #	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Validity
NA	NA	SAASRouter01	70.70.70.1	70	vManage	testZBFW	In Sync	valid

Cisco UTD 버전이 설치되어 있는지 확인합니다.

Router02# show utd engine standard version UTD Virtual-service Name: utd IOS-XE Recommended UTD Version: 1.0.12_SV2.9.16.1_XE17.4 IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.4\$ UTD Installed Version: 1.0.12_SV2.9.16.1_XE17.4 <<<<<<<<

참고 UTD 설치된 버전은 지원되지 않음 상태일 수 없습니다.

UTD가 다음 출력으로 실행 상태인지 확인합니다.

Router02# show app-hosting list App id State utd RUNNING <<<<< 다음 명령은 이전 명령을 요약하고 현재 상태 및 버전을 표시합니다.

Router02# show app-hosting detail appid utd : utd App id Owner : ioxm State : RUNNING ~~~~~~~~~~~~~~~~~~ Application Туре : LXC Name : UTD-Snort-Feature Version : 1.0.12_SV2.9.16.1_XE17.4 <<<<<<<< Description : Unified Threat Defense : /bootflash/.UTD_IMAGES/iox-utd_1.0.12_SV2.9.16.1_XE17.4.tar Path URL Path Activated profile name : cloud-low Resource reservation 2048 MB Momora

Memory	:	204	59	5 MF
Disk	:	861	-	MB
CPU	:			
CPU-percent	:	7 8	5	
VCPU	:	0		

Current signature package version: 29130.156.s

Show utd engine standard status 명령은 UTD 엔진의 상태 및 서명 업데이트를 가져오는 시간을 표시합니다.

Router02# show	v utd eng:	ine standa	rd status	
Engine version	ı :	1.0.6_SV2	.9.13.0_XE17.	2
Profile	:	Cloud-Low	7	
System memory	:			
	Usage :	20.10 %		
	Status :	Green		
Number of engi	nes :	1		
Engine	Running	Health	Reason	
=================				
Engine(#1):	Yes	Green	None	<<<<<<<<
Overall system	n status:	Green	<<<<<<<	
Signature upda	ate status	5:		
=================	===========	===		

Last update status: Successful Last successful update time: Wed Nov 25 07:27:35 2020 EDT <<<<<<< Last failed update time: None Last failed update reason: None Next update scheduled at: None Current status: Idle

다음 명령을 사용하여 활성화된 기능을 확인합니다.

Router02# show platform hardware qfp active feature utd config Global configuration NAT64: disabled Drop pkts: disabled Multi-tenancy: enabled Data plane initialized: yes TLS Decryption Policy: disabled Divert controller mode: enabled SN threads: 12 CFT inst_id 0 feat id 2 fo id 2 chunk id 13 Max flows: 55000 SN Health: channel: Threat Defense : Green SN Health: channel: Service : Down Context Id: 0, Name: Global domain Security Context Ctx Flags: (0x1c70001) Engine: Standard State : Enabled SN Redirect Mode : Fail-open, Divert Threat-inspection: Enabled, Mode: IPS Domain Filtering : Not Enabled URL Filtering : Enabled <<<<<< File Inspection : Enabled <<<<<< All Interfaces : Enabled

일반적인 문제

문제 1. 오류: 다음 장치에 컨테이너 소프트웨어 서비스가 없습니다.

가상 이미지를 활성화합니다.

maintenance(유지 관리) > software(소프트웨어) > activate(활성화)로 이동합니다.

ΰN	IAINTENANCE	SOFTWARE UPGRAD	DE								
WA	N Edge Contro	oller vManage									
1 R	ows Selected	🗩 Upgrade 🛛 O	pgrade Virtual Image 🛛 🗿 Activa	te Virtual li	mage 👔 Delete Vi	rtual Image _ ෆූ	Activate 📑 Dele	ete Available Software	🖉 Set Default V	/ersion	999
Dev	ice Group	· Q	70.70.70.1 ×		Search Options 🗸						Total Rows: 1 of 24
	Hostname			Site ID		Reachability	Current Version		Default Version		Up Since
	SAASRou.	. 70.70.70.1	CSR-FDCDD4AE-4DB9-B79B-8	70	CSR1000v	reachable	17.03.03.0.4762		17.03.03.0.4762	0	05 Nov 2021 11:58:00 AM CST
	•		Activate Virtual Im Following devia Click "Skip Devic • (SAASRd	age ses do not h se' to contin outer01)	iave container softwar ue activate image.	e services.		Skip Devices	×		

가상 이미지에서 오류를 보냅니다. 선택한 **cEdge 라우터에 컨테이너** 프로파일 하위 템플릿의 보안 정책이 없는 경우 디바이스에는 컨테이너 **소프트웨어** 서비스가 없습니다.

Additional Templates			
AppQoE	Choose	•	
Global Template *	Factory Default Global CISCO Template	•	
Cisco Banner	Choose	•	
Cisco SNMP	Choose	•	
CLI Add-On Template	Choose	•	
Policy	Choose	•	
Probes	Choose	•	
Security Policy	CHI Security Policy 2	_	7
Security Policy Please check the Software D	ownload page to ensure your device container versions are up-to-date wi	th the device ver	sion if applicable. It is always recommended that these
are aligned. This is an inform Container Profile * Factor	ative message and no action may be required		

UTD 패키지가 필요한 IPS(Intrusion Prevention System), IDS(Intrusion Detection System), URL 필 터링(URL-F), AMP(Advanced Malware Protection) 등의 보안 기능이 포함된 보안 정책을 사용하는

경우 이 템플릿이 자동으로 추가됩니다. 사용 가능한 모든 보안 기능에 간단한 ZBFW 기능과 같은 UTD 엔진이 필요한 것은 아닙니다.

Add Security Policy

X

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.



컨테이너 프로필 하위 템플릿으로 템플릿을 푸시하면 vmanage에서 자동으로 가상 이미지를 설치 합니다.

문제점 2. 사용 가능한 메모리가 부족합니다.

cEdge 라우터에 8GB DRAM 메모리가 있는지 확인합니다. 그렇지 않은 경우 Lxc 설치 프로세스에 서 **새 컨피그레이션을 허용하도록 디바이스를 전송하지 않습니다. 사용 가능한 메모리 부족** 오류입 니다. cEdge 라우터가 UTD 기능을 사용하려면 최소 8GB의 DRAM이 필요합니다.

TASK VIEW					
Lxc Install Validation Success *				Initiated By: system	From: 1.1
Total Task: 1 Failure : 1					
					0
Q s	Search Options 🗸				Total Rows
Status		Device IP	Message	Start Time	
Y S Failure		70.70.70.2	Failed to install 1/1 lxc countainer (app-hosting-UTD-Snort-Feature-x86_64-1.0	05 Nov 2021 1:31:09 PM	A CST
[5-Nov-2021 19:31:09 UTC] Checking if iox is [5-Nov-2021 19:31:10 UTC] Waiting for iox to [5-Nov-2021 19:31:24 UTC] iox enable	s enabled on device o be enabled on device				
[5-Nov-2021 19:31:24 UIC) Tox enabled on dev [5-Nov-2021 19:31:29 UTC] Failed to install Pre config validation failed. Device is not	vice 1/1 lxc countainer (app configured to accept ne	<pre>-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3). w configuration. Available memory insufficient, required CPU:7 period</pre>	rcent, reserved CPU:0 percent, available CPU:75 percent, required (nemory:2097152 KB, re	ise
				2	

이 경우 CSRv에는 4GB의 DRAM만 있습니다. 메모리를 8GB DRAM으로 업그레이드한 후 성공적 으로 설치되었습니다.

show sdwan system status 출력으로 현재 총 메모리를 확인합니다.

Router01# show sdwan system status

문제 3. 잘못된 참조

보안 정책 시퀀스에 대한 잘못된 참조를 방지하기 위해 보안 정책 기능에 사용되는 VPN/VRF가 cEdge 라우터에 이미 구성되어 있는지 확인합니다.

cisco VManage				
	S			Server error: illegal reference /ncs:devices (device(vip internal temp device CSR-FDCDD4AE-
Device Template testZBFW	Total 1	Config Preview	Config Diff	4DB9-B79B-8FF7-45DF437CBBE0-ec4f8809-8efc- 4461-a182-1c14924618f9)/config/instrative /ip/access-list/extended{GCP_Out_v06_copy-
Device list (Total: 1 devices) Filter/Search				seq-38674_GCP_SQL_RULE-acl_//access-list-seq- rule{11}/ace-rule/object-group
CSR-FDCDD4AE-4DB9- B79B-8FF7-45DF437CBBE0 SAASRouter01 70.70.70.1				

이 예에서 보안 정책에는 VPN/VRF 1에 대한 침입 방지 정책이 있지만 디바이스에는 구성된 VRF 1이 없습니다. 따라서 vmanage에서 해당 정책 시퀀스에 대한 잘못된 참조를 보냅니다.

	Edit Intrusion Prevention Policy			
	Target		Policy Behavior	
		Inspection Mode: Detection	Signature Set: Security Whitelist: -	Log Level: Warning
	Target VPNs	Actions	Signatures	Alerts
Intrusion Prevention -	Policy Rule Configuration	•		
Policy Name	GPC_IPS_v06_copy_copy			
Signature Set	Security	• Inspection	Mode Detection	×
Advanced >				

보안 정책에서 언급한 VRF를 구성한 후에는 잘못된 참조가 나타나지 않으며 템플릿이 성공적으로 푸시됩니다.

문제 4. UTD가 설치되어 있고 활성화되어 있지만 활성화되지 않았습니다.

디바이스에 보안 정책이 구성되어 있고 UTD가 설치되어 있고 활성화되어 있지만 활성화되지 않았 습니다.

이 문제는 문제 번호 3과 관련이 있습니다. 그러나 vManage에서는 컨피그레이션이 디바이스에 구 성되지 않은 VRF를 참조하도록 허용했으며 정책이 어떤 VRF에도 적용되지 않았습니다.

라우터에 이 문제가 있는지 확인하려면 UTD가 활성 상태인지를 확인해야 합니다. UTD가 활성화되 지 않음 메시지 및 정책이 VRF를 참조하지 않습니다. UTD engine standard is not enabled <<<<<<

ISR01#show sdwan virtual-application utd

VERSION

ACTIVE PREVIOUS

TIMESTAMP

1.0.16_SV2.9.16.1_XE17.3truetrue2022-06-10T13:29:43-00:00해결을 위해 대상 VPN을 확인하고 구성된 VRF에 정책을 적용해야 합니다.

관련 정보

- <u>라우터 보안: 라우터의 Snort IPS</u>
- <u>Cisco SD-WAN 보안 컨피그레이션 가이드, Cisco IOS XE 릴리스</u>
- <u>기술 지원 및 문서 Cisco Systems</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.