Cisco Umbrella와의 통합 구성 및 일반적인 문제 해결

목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>구성</u> <u>확인 및 문제 해결</u> <u>클라이언트 확인</u> <u>cEdge 확인</u> <u>Umbrella의 EDNS 구현 이해</u> <u>vManage 대시보드에서 확인</u> <u>DNS 캐싱</u> <u>보안 DNS</u> 결론

소개

이 문서에서는 Cisco Umbrella DNS 보안 솔루션과의 통합에서 vManage/Cisco IOS®-XE SDWAN 소프트웨어 부분에 대해 설명합니다.그러나 Umbrella 정책 컨피그레이션 자체는 다루지 않습니다 .Cisco Umbrella에 대한 자세한 내용은 https://docs.umbrella.com/deploymentumbrella/docs/welcome-to-cisco-umbrella을 참조하십시오.

참고:이미 Umbrella 서브스크립션을 획득하고 cEdge 라우터 컨피그레이션에 사용할 Umbrella 토큰을 가져와야 합니다.API 토큰에 대한 자세한 정보: <u>https://docs.umbrella.com/umbrella-api/docs/overview2.</u>

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• vManage 18.4.0

• Cisco IOS®-XE SDWAN 라우터 실행(cEdge) 16.9.3

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

구성

Cisco Umbrella와의 cEdge 통합을 구성하려면 vManage에서 다음과 같은 간단한 단계를 수행합니 다.

1단계. Congistration(**컨피그레이션) > Security(보안)**에서 **Custom Options(맞춤형 옵션**) 드롭다운 목록을 오른쪽 상단 모서리에서 **선택한** 다음 Umbrella **API 토큰을 선택합니다**.이미지에 표시된 대 로 Umbrella 등록 토큰을 입력합니다.

Manage Umbrella Registration		×
Registration Token	FE5540@DE14849@#88003@646664@5824@684	
	Save Changes Cancel	

또는 vManage 소프트웨어 20.1.1 릴리스부터 Organization ID, Registration Key 및 Secret을 지정 할 수 있습니다.Administration(관리) > Settings(설정) > Smart Account Credentials(**Smart Account 자격 증명**)에서 Smart Account 자격 증명을 구성한 경우 이러한 매개변수를 자동으로 검색할 수 있 습니다.

Cisco Umbrella Registration Key and Secret 0

Organization ID	Enter Organization ID	ĺ
Registration Key	Enter Registration Key	
Secret	Enter Secret	
	Get Keys	
Cisco Umbrella Regis	tration Token 🕕	
-,		/

Cancel

2단계. Configuration > Security에서 Add Security Policy(보안 정책 추가)를 선택한 다음 이미지에 표시된 대로 사용 사례에 맞는 시나리오(예: 사용자 지정)를 선택합니다.

Add Security Choose a s	cenario that fits your use-case. Click Proceed to continue building your desired policies.
≡,∕	Compliance Application Firewall Intrusion Prevention
**	Guest Access Application Firewall URL Filtering
ø	Direct Cloud Access Application Firewall Intrusion Prevention Umbrella DNS Security
	Direct Internet Access Application Firewall Intrusion Prevention URL Filtering Umbrella DNS Security
٩	Custom Build your ala carte policy by combining a variety of security policy blocks
	Proceed Cancel

3단계. 이미지에 표시된 대로 DNS Security(DNS 보안)로 이동하고 Add DNS Security Policy(DNS 보안 정책 추가)를 선택한 다음 Create New(새로 만들기)를 선택합니다.



화면에 표시되는 이미지와 비슷한 화면이 나타납니다.

🚖 Cisco vManage			٠	69	•	0	admin •
CONFIGURATION SECURITY	Add DNS Security Policy						
Target		Policy Behavior					
ALL -	Domain Liat: •	VPNs Attached ALL DNS Server: Underella Default	-	Report	ation: Un	nbrella Del	ndi .
C Target 1979a	Local Domain Bypass	Action		Umbr	ella Reg	istration	
DNS Security - Policy I	Rule Configuration						
Pallop Name	Maximum of 22 characters						
NucchAllyph O D	GP Contigured Controls magistration						
Local Domain Bypess List	Solect a Domain list.						
DNS Server IP	() Unberlaßefest O Custom DNS	Server P					
Advanced >							
	Save DNS Securit	Poky Contra					

4단계. 구성되면 표시되는 이미지.

Cisco vManage						•	Ê	4 20	Ø	adm	nin 🔻
CONFIGURATION Sec	urity > View Security	y Policy Securi	ty-Policy-2						III Custon	n Option	s -
	Firewall	Intrusion Pre	evention	URL Filtering	DNS Security	Policy	y Summary				
										0	
۹		Searc	h Options 🥆	/						Total Ro	ws: 1
Name	Туре	R	eference (Count	Updated By			Last Updat	ed		
DNS-Security-Policy-2	c dnsSecurity	1			admin			20 Nov 201	8 4:31:36 P	PM P	•••

5단계. **...> View(보기) > DNS Security(DNS 보안**) 탭으로 이동하여 다음 이미지와 유사한 컨피그레 이션이 표시됩니다.

=	cisco vManage			•	ê 🍂	²⁰ Ø	admin 🔻
::		/iew DNS Security Policy				III Custom C	Options 👻
	Target		Policy Behavior				
* *	ALL -	Domain List: domainbypasslist	VPNs Attached: ALL DNS Server: Umbrella Default	-	Registration:	Umbrella Defau	lt
4	VPNs	Local Domain Bypass	Action		Umbrella	Registration	
•	DNS Security - Policy R	ule Configuration 🏮					
	Policy Name	DNS-Security-Policy-2					
	Umbrella Registration Status:	Configured					
	Match All VPN O Cus	stom VPN Configuration					
	Local Domain Bypass List	domainbypasslist	¥				
	DNS Server IP	Umbrella Default O Custom DNS	Server IP				
	Advanced >						

"Local Domain Bypass List"는 라우터가 DNS 요청을 Umbrella 클라우드로 리디렉션하지 않고 DNS 요청을 특정 DNS 서버(엔터프라이즈 네트워크 내에 있는 DNS 서버)로 전송하는 도메인 목록 입니다. 이는 Umbrella 보안 정책에서 제외되지 않습니다.특정 카테고리의 일부 도메인을 "화이트 리스트"하려면 대신 Umbrella 컨피그레이션 포털에서 제외를 구성하는 것이 좋습니다.

또한 CLI에서 컨피그레이션이 어떻게 표시되는지 파악하기 위해 Preview를 선택할 수 있습니다.

```
policy
 lists
  local-domain-list domainbypasslist
    cisco.com
  !
 1
1
exit
!
security
 umbrella
  token XFFFX543XDF14X498X623CX222X4CCAX0026X88X
  dnscrypt
!
exit
!
vpn matchAllVpn
 dns-redirect umbrella match-local-domain-to-bypass
```

6단계. 이제 디바이스 템플릿에서 정책을 참조해야 합니다.Configuration > Templates에서 컨피그 레이션 템플릿을 선택하고 이미지에 표시된 Additional Templates 섹션에서 참조합니다.

=	Cisco vManage				•	Ċ.		•	admin •
	CONFIGURATION TEMPLATES								
	Basic Information	Transport & Management VPN	Service VPN	Cellular	Additional Temp	lates			
٠	Additional Templates								
1	Barner	Okoner_	*						
	Pelky	005400041857	٠						
•	SHMP	Choose.							
	Security Policy	Security Policy-2							

7단계. 디바이스에 템플릿을 적용합니다.

확인 및 문제 해결

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인하고 문제를 해결하십시오.

클라이언트 확인

cEdge 뒤에 있는 클라이언트에서 다음 테스트 사이트를 탐색할 때 Umbrella가 제대로 작동하는지 확인할 수 있습니다.

- <u>http://welcome.opendns.com</u>
- <u>http://www.internetbadguys.com</u>

자세한 내용은 <u>방법:Umbrella가 제대로 실행되고 있는지 테스트했습니다.</u>

cEdge 확인

cEdge 자체에서도 확인 및 문제 해결을 수행할 수 있습니다.일반적으로 Cisco 4000 Series ISRs of Security Configuration Guide 2장의 Cisco Umbrella Integration에서 찾을 수 있는 Cisco IOS-XE 소 프트웨어 통합 문제 해결 절차와 유사합니다.Cisco Umbrella Integration, Cisco IOS-XE Fuji 16.9.x: <u>https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_umbrbran/configuration/xe-16-9/sec-data-umbrella-branch-xe-16-9-book.pdf.</u>

확인할 수 있는 몇 가지 유용한 명령:

1단계. 매개변수 맵이 디바이스의 cEdge 컨피그레이션에 표시되는지 확인합니다.

```
dmz2-site201-1#show run | sec parameter-map type umbrella
parameter-map type umbrella global
token XFFFX543XDF14X498X623CX222X4CCAX0026X88X
local-domain domainbypasslist
dnscrypt
udp-timeout 5
vrf 1
dns-resolver umbrella
match-local-domain-to-bypass
```

Cisco IOS-XE에서 이 매개변수 맵을 보는 데 사용되므로 인터페이스에서 이 매개변수 맵에 대한 참 조를 찾을 수 없습니다.

이는 매개변수 맵이 인터페이스가 아닌 VRF에 적용되기 때문에 여기에서 확인할 수 있습니다.

```
dmz2-site201-1#show umbrella config
Umbrella Configuration
_____
  Token: XFFFX543XDF14X498X623CX222X4CCAX0026X88X
  OrganizationID: 2525316
  Local Domain Regex parameter-map name: domainbypasslist
  DNSCrypt: Enabled
  Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
  UDP Timeout: 5 seconds
  Resolver address:
      1. 208.67.220.220
      2. 208.67.222.222
      3. 2620:119:53::53
      4. 2620:119:35::35
  Registration VRF: default
  VRF List:
      1. VRF 1 (ID: 2)
          DNS-Resolver: umbrella
          Match local-domain-to-bypass: Yes
```

또한 이 명령을 사용하여 자세한 정보를 얻을 수 있습니다.

dmz2-site201-1#show platform hardware qfp active feature umbrella client config
+++ Umbrella Config +++

Umbrella feature:

Init: Enabled Dnscrypt: Enabled

Timeout:

udp timeout: 5

Orgid:

orgid: 2525316

Resolver config:

RESOLVER IP's 208.67.220.220

208.67.222.222 2620:119:53::53 2620:119:35::35 Dnscrypt Info: _____ public_key: A7:A1:0A:38:77:71:D6:80:25:9A:AB:83:B8:8F:94:77:41:8C:DC:5E:6A:14:7C:F7:CA:D3:8E:02:4D:FC:5D:21 magic_key: 71 4E 7A 69 6D 65 75 55 serial number: 1517943461 Umbrella Interface Config: _____ 09 GigabitEthernet0/0/2 : Mode : IN DeviceID : 010aed3ffebc56df : vpn1 Tag 10 Loopback1 : : IN Mode DeviceID : 010aed3ffebc56df Tag : vpn1 08 GigabitEthernet0/0/1 : Mode : OUT 12 Tunnell : : OUT Mode Umbrella Profile Deviceid Config: _____ ProfileID: 0 Mode : OUT ProfileID: 2 Mode : IN Resolver : 208.67.220.220 Local-Domain: True DeviceID : 010aed3ffebc56df Tag : vpn1 Umbrella Profile ID CPP Hash: _____ VRF ID :: 2 VRF NAME : 1 Resolver : 208.67.220.220 Local-Domain: True _____ 2단계. 장치가 Umbrella DNS 보안 클라우드에 성공적으로 등록되었는지 확인합니다.

dmz2-site201-1#show umbrella deviceidDevice registration detailsVRFTag1vpn1200 success010aed3ffebc56df3단계. 다음은 우산 DNS 리디렉션 통계를 확인하는 방법입니다.

dmz2-site201-1#show platform hardware qfp active feature umbrella datapath stats Umbrella Connector Stats: Parser statistics: parser unknown pkt: 12991 parser fmt error: 0 parser count nonzero: 0 parser pa error: 0 parser non query: 0 parser multiple name: 0 parser dns name err: 0 parser matched ip: 0 parser opendns redirect: 1234 local domain bypass: 0 parser dns others: 9 no device id on interface: 0 drop erc dnscrypt: 0 regex locked: 0 regex not matched: 0 parser malformed pkt: 0 Flow statistics: feature object allocs : 1234 feature object frees : 1234 flow create requests : 1448 flow create successful: 1234 flow create failed, CFT handle: 0 flow create failed, getting FO: 0 flow create failed, malloc FO : 0 flow create failed, attach FO : 0 flow create failed, match flow: 214 flow create failed, set aging : 0 flow lookup requests : 1234 flow lookup successful: 1234 flow lookup failed, CFT handle: 0 flow lookup failed, getting FO: 0 flow lookup failed, no match : 0 flow detach requests : 1233 flow detach successful: 1233 flow detach failed, CFT handle: 0 flow detach failed, getting FO: 0 flow detach failed freeing FO : 0 flow detach failed, no match : 0 flow ageout requests : 1 flow ageout failed, freeing FO: 0 flow ipv4 ageout requests : 1 flow ipv6 ageout requests : 0 flow update requests : 1234 flow update successful: 1234 flow update failed, CFT handle: 0 flow update failed, getting FO: 0 flow update failed, no match : 0 DNSCrypt statistics: bypass pkt: 1197968 clear sent: 0 enc sent: 1234 clear rcvd: 0 dec rcvd: 1234 pa err: 0 enc lib err: 0 padding err: 0 nonce err: 0 flow bypass: 0 disabled: 0

```
flow not enc: 0
DCA statistics:
   dca match success: 0
   dca match failure: 0
```

4단계. ping 및 traceroute와 같은 문제를 해결하려면 일반 도구를 사용하여 DNS 확인자에 연결할 수 있는지 확인합니다.

5단계. Cisco IOS-XE의 임베디드 패킷 캡처를 사용하여 cEdge에서 전송되는 DNS 패킷 캡처를 수 행할 수도 있습니다.

자세한 내용은 컨피그레이션 가이드(https://www.cisco.com/c/en/us/td/docs/iosxml/ios/epc/configuration/xe-16-9/epc-xe-16-9-book/nm-packet-capture-xe.html)을 <u>참조하십시오.</u>

Umbrella의 EDNS 구현 이해

패킷 캡처를 수행한 후 DNS 쿼리가 올바른 EDNS0(DNS용 확장 메커니즘) 정보를 사용하여 Umbrella DNS 확인기로 올바르게 리디렉션되었는지 확인합니다. SD-WAN Umbrella DNS 레이어 검사 통합을 통해 cEdge 장치는 Umbrella DNS 확인으로 DNS 쿼리를 보낼 때 ENDS0 옵션을 포함 합니다.이러한 확장에는 DNS 쿼리에 응답할 때 사용할 올바른 정책을 식별하기 위해 Umbrella에서 수신하는 장치 ID cEdge 및 Umbrella의 조직 ID가 포함됩니다.다음은 EDNS0 패킷 형식의 예입니 다.

 Additional records 	
<pre>v <root>: type OPT</root></pre>	
Name: <root></root>	
Type: OPT (41)	
UDP payload size: 512	
Higher bits in extended RCODE: 0x00	
EDNS@ version: 0	
0 = D0 bit: Cannot handle DNSSEC security RR .000 0000 0000 0000 = Reserved: 0x0000	5
Data length: 39	
v Option: Unknown (26946)	
Option Code: Unknown (26946)	
Option Length: 15	
Option Data 4f70656e444e53010afb86c9fb1aff	
v Option: Unknown (20292)	
Option Code: Unknown (20292)	
Option Length: 16	
Option Data: 4f444e5300000800225487100b010103	

옵션 분류는 다음과 같습니다.

RDATA 설명:

0x4f70656e444e53: Data ="OpenDNS" 0x10afb86c9b1aff: Device-ID RDATA 원격 IP 주소 옵션:

0x4f444e53: MGGIC = 'ODNS' 0x00 : Version 0x00 : Flags 0x08 : Organization ID Required 0x00225487: Organization ID 0x10 type : Remote IPv4 0x0b010103: Remote IP Address = 11.1.1.3 Device-ID가 올바른지 확인하고 Organization ID가 Umbrella 포털과 Umbrella 어카운트와 일치하는 지 확인합니다. **참고:**DNSCrypt를 활성화하면 DNS 쿼리가 암호화됩니다.패킷이 Umbrella 확인자로 이동하 는 DNScrypt 패킷을 보여주지만 반환 트래픽이 없는 경우 DNSCrypt를 비활성화하여 문제가 있는지 확인합니다.

vManage 대시보드에서 확인

모든 Cisco Umbrella 지정 트래픽은 vManage 대시보드에서 볼 수 있습니다.[**모니터] > [네트워크] >** [Umbrella DNS 재다이렉트]에서 볼 수 있습니다. 이 페이지의 이미지는 다음과 같습니다.

MONITOR Network > Umbrella DNS Re-direct								
Select Device -	CSR_cEdge8 23.1.1.8 Site ID: 238 Device M	todel: CSR1000# 👴						
Interface	Limburilla Danietanad VDMe		2/6	DMOCOUNT Backle				
QuS	ornoreia Registereo VENs		2/0	очостурт. влане	Last Updated: 14 Jun 2828 11			
TCP Optimization			Local Domain Bypass	DNS Re-direct				
WAN Throughput					1h 3h 6h 12h 24h 7days Custom •			
Flows								
Top Talkera	E A			Jun 14, 20:40:00 • prop: 2				
WAN	8 2 V	٨	٨	*				
TLOC		\wedge	\wedge					
Tunnel	0 Jun 14, 18:45 Jun 14, 19:00	Jun 14, 19:15 Jun 14, 19:10 Jun 14, 1	9.45 Jun 14, 20:00	Jun 14, 20:15 Jun 14, 20:30 Jun 14, 20:45	Jun 14, 21:00 Jun 14, 21:15 Jun 14, 21:10			
Security Monitoring								
Firewall					00			
Intrusion Prevention	Q	Search Options 👻			Total Rows: 37			
URL Filtering	Timestamp	Packet Co	unt					
Advanced Malware	14 Jun 2020 8:45:00 PM PDT	0						
Protection	14 Jun 2020 8:40:00 PM PDT	2						
TLS/SSL Decryption	14 Jun 2020 8:35:00 PM PDT	0						
Umbrella DNS Re-direct								

DNS 캐싱

Cisco cEdge 라우터에서 로컬 도메인 우회 플래그가 일치하지 않는 경우도 있습니다.이는 호스트 시스템/클라이언트에 캐싱이 포함된 경우 발생합니다.예를 들어, 로컬 도메인 우회가 www.cisco.com과 일치하고 우회하도록 구성된 경우(**.*cisco.com**). 처음 쿼리는 www.cisco.com에 대한 것이며 <u>CDN</u> 이름을 CNAME으로 반환했으며, 이는 클라이언트에 캐시되었습니다 .www.cisco.com에 대한 nslookup에 대한 후속 쿼리는 CDN 도메인(akamaiedge)에 대한 쿼리만 전 송했습니다.

Non-authoritative answer: www.cisco.com canonical name = www.cisco.com.akadns.net. www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net. wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e2867.dsca.akamaiedge.net. Name: e2867.dsca.akamaiedge.net Address: 104.103.35.55 Name: e2867.dsca.akamaiedge.net Address: 2600:1408:8400:5ab::b33 Name: e2867.dsca.akamaiedge.net Address: 2600:1408:8400:59c::b33 Z컬 도메인 우회가 제대로 작동하는 경우 파서 OpenDNS 리디렉션에 대한 카운터가 증가함을 확 인할 수 있습니다. 다음은 약식 출력입니다. dmz2-site201-1#show platform hardware qfp active feature umbrella datapath stats Umbrella Connector Stats:

이는 로컬 도메인 우회가 라우터에서 보이지 않는 이유일 수 있습니다.호스트/클라이언트 시스템에 서 캐시를 지우면 쿼리가 올바르게 로그아웃됩니다.

보안 DNS

Google Chrome과 같은 최신 브라우저는 버전 83부터 HTTPS를 통한 DNS(DoH) 또는 DoT(DNS over TLS)라고도 하는 Secure DNS를 사용하고 있습니다. 이 기능을 사용하면 신중하게 계획하지 않은 경우 Umbrella DNS 보안 기능을 사용할 수 없습니다.보안 DNS는 중앙 집중식 정책을 통해 비 활성화할 수 있으며, 예를 들어 엔터프라이즈 관리 컴퓨터의 경우 기본적으로 비활성화할 수 있습 니다.

Settings		Q DNS	⊗
+	You and Google	Use secure DNS	
Ê	Auto-fill	This setting is disabled on managed browsers	

관리되지 않는 BYOD 장치에는 몇 가지 옵션이 있습니다.첫 번째 옵션은 Secure DNS에서 사용하는 TCP 포트 853을 차단하는 것입니다.이 용도로 Cisco ZBFW(Zone Based Firewall)를 사용할 수 있습니다.두 번째 옵션은 Umbrella 포털에서 "Proxy/Anonyizer" 카테고리 차단을 활성화하는 것입니다.자세한 내용은 여기를 참조하십시오.

https://support.umbrella.com/hc/en-us/articles/360001371526-Web-Browsers-and-DNS-over-HTTPS-default

결론

보시다시피 Umbrella DNS 보안 클라우드와 통합은 cEdge에서 매우 간단하며 몇 분 만에 완료할 수 있습니다.