Cisco Umbrellaとの統合の設定と一般的な問題の トラブルシューティング

内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント</u> <u>設定</u> 確認とトラブルシューティング クライアントの検証 <u>cEdgeの検証</u> <u>UmbrellaのEDNS実装の理解</u> <u>vManageダッシュボードで確認します。</u> <u>DNSキャッシュ</u> <u>セキュアDNS</u> 結論

概要

このドキュメントでは、Cisco Umbrella DNSセキュリティソリューションとの統合の vManage/Cisco IOS® -XE SDWANソフトウェア部分について説明します。ただし、Umbrellaポリ シーの設定自体はカバーしていません。Cisco Umbrellaの詳細については、 https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrellaを参照<u>してくださ</u> い。

注:cEdgeルータの設定で使用されるUmbrellaサブスクリプションを取得し、Umbrellaトー クンを取得する必要があります。APIトークンの詳細:<u>https://docs.umbrella.com/umbrella-</u> <u>api/docs/overview2</u>

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

• vManage 18.4.0

• (cEdge)16.9.3が稼働するCisco IOS® -XE SDWANルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

設定

Cisco UmbrellaとのcEdge統合を設定するには、vManageで一連の簡単な手順を実行します。

ステップ1:[Congifuration] > [Security]で、右上隅の[Custom Options]ドロップダウンリストを選択し、[Umbrella API token]を選択します。図に示すように、Umbrella登録トークンを入力します。

Manage Umbrella Registration		×
Registration Token	FE55-0300E1494900080003004400088400884	
	Save Changes Cancel	

または、vManageソフトウェア20.1.1リリース以降では、組織ID、登録キー、およびシークレットを指定できます。これらのパラメータは、[管理(Administration)] > [設定(Settings)] > [スマートアカウントのクレデンシャル(Smart Account Credentials)]でスマートアカウントのクレデンシャルルを設定した場合に自動的に取得できます。

Cisco Umbrella Registration Key and Secret 0

Registration Key	Enter Registration Key	
iecret	Enter Secret	
	Get	Keys

egistration Token Must be exactly 40 hexadecimal characters	Registration Token Must be exactly 40 hexadecimal characters			
		Registration Token	Must be exactly 40 hexadecimal characters	

ステップ2:[Configuration] > [Security] で、[Add Security Policy] を選択し、次に図に示すように、 使用例(カスタムなど)に合うシナリオを選択します。

Add Security	Policy X
Choose a so	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

ステップ3 : 図に示すように、[DNS Security]に移動し、[**Add DNS Security Policy**]を選択し、 [Create New]を選択します。



次のような画面が表示されます。

dirde Cisco vManage			•	69		0	admin *
CONFIGURATION SECURITY	Add DNS Security Policy						
Target		Policy Behavior					
ALL -	Demain List: -	VPNo Attached ALL DNS Server: Underella Default	-	Registra	tor: Uni	rella Della	ult
C Tarpet 1979a	Local Domain Bypass	Action		Umbre	illa Regis	tration	
DNS Security - Policy F	Nule Configuration 🧿						
Pallop Name	Maximum of 22 characters						
Unbrella Registration Status:	O Configured Umbrella Registration						
NVICE ALLYPH O	atom VPN Configuration						
Local Domain Bypass List	Soled a Domain list.						
DNS Server IP	() Unbrelie befault () Custom DNS	Server P					
Advanced >							
	Save DNS Securit	Poky CANCEL					

ステップ4:これは、設定後の表示方法のイメージです。

Cisco vManage				•	• Ê	<u></u> ²⁰	? ac	lmin 🔻
CONFIGURATION Security > View Security Policy Security-Policy-2								ons 👻
	Firewall	trusion Prevention	URL Filtering	DNS Security	Policy Summar	у		
							(
Q		Search Options 🗸	·				Total I	Rows: 1
Name	Туре	Reference C	Count	Updated By		Last Updated	I	
DNS-Security-Policy-2	c dnsSecurity	1		admin		20 Nov 2018	4:31:36 PM P	•••

ステップ5 : ポリシーの[**...]> [View] > [DNS Security]**タブに移動します。次の図のような設定が表 示されます。

≡	cisco VManage			•	Ê .	≜ 20	0	admin 👻
::		View DNS Security Policy					Custom (Options 👻
	Target		Policy Behavior					
ت عر	ALL -	Domain List: domainbypasslist	VPNs Attached: ALL DNS Server: Umbrella Default		Registratio	n: Um	ıbrella Defau	ult
₽ .::	VPNs	Local Domain Bypass	Action		Umbrell	a Regi	stration	
•	DNS Socurity - Policy P	ula Configuration						
	DNS Security - Policy R							
	Policy Name	DNS-Security-Policy-2						
	Umbrella Registration Status:	Configured						
	Match All VPN O Cu	stom VPN Configuration						
	Local Domain Bypass List	domainbypasslist	*					
	DNS Server IP	O Umbrella Default O Custom DNS	Server IP					
	Advanced >							

「ローカルドメインバイパスリスト」は、ルータがDNS要求をUmbrellaクラウドにリダイレクト せず、特定のDNSサーバ(企業ネットワーク内にあるDNSサーバ)にDNS要求を送信するドメイ ンのリストであり、Umbrellaセキュリティポリシーからは除外されないことに注意してください 。特定のカテゴリの一部のドメインを「ホワイトリスト」にするには、代わりにUmbrella設定ポ ータルで除外を設定することをお勧めします。

また、CLIでの設定の外観を理解するために[Preview]を選択することもできます。

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

ステップ6:次に、デバイステンプレートでポリシーを参照する必要があります。[設定] > [テンプ レート]で、設定テンプレートを選択し、図に示すように[追加テンプレート]セクションで参照し ます。

=	citos Cisco vManage				•	۵	*	0	admin •
	CONFIGURATION TOWN	LATES							
	Basic Information	Transport & Management VPN	Service VPN	Collular	Additional Temp	laten			
۰	Additional Templates								
٩	Bawer	Ohones	*						
۰									
45.	Parky	CORPOUCH TEST							
	State.	Choose.							
	Security Policy	Security-Policy-2							

ステップ7:デバイスにテンプレートを適用します。

確認とトラブルシューティング

このセクションでは、設定が正しく動作していることを確認し、トラブルシューティングを行い ます。

クライアントの検証

cEdgeの背後にあるクライアントから、次のテストサイトを参照するときにUmbrellaが正しく動 作するかどうかを確認できます。

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

詳細は、『<u>How To:Umbrellaが正しく実行されていることを確認するためのテストが正常に完了</u> しました

cEdgeの検証

検証とトラブルシューティングは、cEdge自体でも実行できます。一般的には、Cisco IOS-XEソ フトウェアの統合に関するトラブルシューティング手順に似ていますが、『セキュリティ設定ガ イド』の第2章「Cisco 4000シリーズISRでのCisco Umbrella統合」に記載されています。Cisco Umbrella統合、Cisco IOS-XE Fuji 16.9.x:<u>https://www.cisco.com/c/en/us/td/docs/ios-</u> <u>xml/ios/sec_data_umbrbran/configuration/xe-16-9/sec-data-umbrella-branch-xe-16-9-book.pdf</u>

確認する便利なコマンドがいくつかあります。

ステップ1:デバイスのcEdge設定にパラメータマップが表示されることを確認します。

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

1

Cisco IOS-XEでこのパラメータマップを表示するのに慣れているので、インターフェイスでこの パラメータマップへの参照が見つかりません。

これは、パラメータマップがVRFに適用され、インターフェイスには適用されないためです。こ こで確認できます。

```
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
```

さらに、次のコマンドを使用して詳細情報を取得できます。

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 Tag : vpnl 10 Loopback1 : : IN Mode DeviceID : 010aed3ffebc56df Tag : vpnl 08 GigabitEthernet0/0/1 : Mode : OUT 12 Tunnell : Mode : OUT Umbrella Profile Deviceid Config: -----ProfileID: 0 Mode : OUT ProfileID: 2 : IN Mode 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 -----ステップ2:デバイスがUmbrella DNS Securityクラウドに正常に登録されていることを確認しま

す。

Device registration detailsVRFTagStatusDevice-id1vpn1200 success010aed3ffebc56dfステップ3:傘のDNSリダイレクト統計情報を確認する方法を次に示します。

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
```

ステップ4:pingやtracerouteなどのトラブルシューティングを行うために、汎用ツールを使用して DNSリゾルバに到達できることを確認します。

ステップ5:Cisco IOS-XEのEmbedded Packet Capture(EPC)を使用して、cEdgeから送信される DNSパケットキャプチャを実行することもできます。

詳細については、構成ガイド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を参照してく<u>ださ</u> い<u>。</u>

UmbrellaのEDNS実装の理解

パケットキャプチャが行われた後で、DNSクエリがUmbrella DNSリゾルバー(208.67.222.222お よび208.67.220.220、正しいEDNS0(DNS拡張メカニズム)情報に正しくリダイレクトされるこ とを確認します。SD-WAN Umbrella DNSlayerinspectionintegration解決これらの拡張機能には、 Umbrellaから受信したデバイスID cEdgeと、DNSクエリの応答時に使用される正しいポリシーを 識別するためのUmbrellaの組織IDが含まれます。EDNS0パケット形式の例を次に示します。

▼ 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
- Z: 0x0000
0 = D0 bit: Cannot handle DNSSEC security RRs .000 0000 0000 = Reserved: 0x0000
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: 4f444e53000000800225487100b010103

オプションの内訳を次に示します。

RDATAの説明:

0x4f70656e444e53: Data ="OpenDNS" 0x10afb86c9b1aff: Device-ID RDATAリモートIPアドレスオプション:

0x4f444e53: MGGIC = 'ODNS' 0x00 : Version 0x00 : Flags 0x08 : Organization ID Required 0x00225487: Organization ID デバイスIDが正しく、組織IDがUmbrellaポータルを使用してUmbrellaアカウントと一致している ことを確認します。

注:DNSCryptを有効にすると、DNSクエリが暗号化されます。パケットキャプチャで Umbrellaリゾルバに向かうDNScryptパケットが示されている場合にリターントラフィック がない場合は、DNSCryptを無効にして問題があるかどうかを確認してください。

vManageダッシュボードで確認します。

Cisco Umbrella宛てのトラフィックは、vManageダッシュボードから表示できます。[**Monitor**] > [**Network**] > [**Umbrella DNS Re-direct**]で表示できます。次に、このページのイメージを示します。



DNSキャッシュ

Cisco cEdgeルータでは、ローカルドメインバイパスフラグが一致しないことがあります。これ は、ホストマシン/クライアントにキャッシュが含まれている場合に発生します。たとえば、ロー カルドメインバイパスがwww.cisco.com(**.*cisco.com**)に一致してバイパスするように設定されて いる場合は、ローカルドメイ**ンバイパスが使用さ**れます。 最初にクエリは<u>www.cisco.com</u>に対し て行われ、クライアントでキャッシュされたCDN名もCNAMEとして返されました。 www.cisco.comのnslookupに対する後続のクエリ<u>は、</u>CDNドメイン(akamaiedge)に対するクエリ のみを送信することでした。

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. wwwds.cisco.com.edgekey.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

ローカルドメインバイパスが正常に動作している場合は、パーサーOpenDNSリダイレクトのカウ ンタが増加していることがわかります。これは省略された出力です。

dmz2-site201-1#show platform hardware qfp active feature umbrella datapath stats Umbrella Connector Stats: Parser statistics: parser unknown pkt: 0 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: 3 local domain bypass: 0 <<<<<<<</pre>

これは、ローカルドメインバイパスがルータに表示されない理由である可能性があります。ホスト/クライアントマシンのキャッシュをクリアすると、クエリが正しく送信されていることがわかります。

セキュアDNS

Google Chromeなどの最新のブラウザは、DNS over HTTPS(DoH)またはDNS over TLS(DoT)と も呼ばれるセキュアDNSを使用しています。この機能により、Umbrella DNSセキュリティ機能が 慎重に計画されていない場合使用できなくなります。Secure DNSは、中央集中型ポリシーを使用 して無効にすることも、エンタープライズ管理コンピューターの場合など、デフォルトで無効に することもできます。

Setti	ngs	Q DNS	8
÷	You and Google	Use secure DNS	
Ê	Auto-fill	This setting is disabled on managed browsers	

管理対象外のBYODデバイスには、いくつかのオプションがあります。最初のオプションは、 Secure DNSで使用されるTCPポート853をブロックすることです。この目的には、Cisco Zone Based Firewall(ZBFW)を使用できます。2つ目のオプションは、Umbrellaポータルで「プロキシ /匿名化」カテゴリのブロックを有効にすることです。詳細については、こちらを参照してくださ い

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

結論

ご覧のように、Umbrella DNSセキュリティクラウドとの統合はcEdge側から非常にシンプルで、 数分で完了できます。