使用CLI和ASDM配置ASA資料包捕獲

目錄

簡介 必要條件 需求 採用元件 背景資訊 設定 網路圖表 組態 使用ASDM配置資料包捕獲 使用CLI配置資料包捕獲 ASA上的可用捕獲型別 預設值 檢視捕獲的資料包 在ASA上 從ASA下載以進行離線分析 清除捕獲 停止捕獲 驗證 疑難排解

簡介

本文檔介紹如何配置Cisco ASA防火牆以使用ASDM或CLI捕獲所需資料包。

必要條件

需求

此過程假定ASA完全可以運行並且已進行配置以允許Cisco ASDM或CLI進行配置更改。

採用元件

本檔案所述內容不限於特定硬體或軟體版本。

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

相關產品

此組態也會用於以下思科產品:

- Cisco ASA 9.1(5)及更高版本
- Cisco ASDM版本7.2.1

背景資訊

本檔案介紹如何設定 Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall 以便使用 Cisco Adaptive Security Device Manager (ASDM) 或 Command Line Interface (CLI) (ASDM).

資料包捕獲過程對於排除連線問題或監控可疑活動非常有用。此外,還可以建立多個捕獲,以便分 析多個介面上不同型別的流量。

設定

本節提供的資訊用於設定本檔案中所述的封包擷取功能。

網路圖表

本檔案會使用以下網路設定:



192.168.10.10/24

組態

此配置中使用的IP地址方案在Internet上不能合法路由。它們是實驗室環境中使用的RFC 1918地址。

使用ASDM配置資料包捕獲

以下範例組態用於擷取從User1(內部網路)對Router1(外部網路)執行ping期間傳輸的封包。

完成以下步驟,以便使用ASDM在ASA上配置資料包捕獲功能:

1.定位至 Wizards > Packet Capture Wizard 要啟動資料包捕獲配置,如下所示:



2. Capture Wizard 開啟。按一下 Next.

Capture Wizard	
Packet Capture Wizard	Overview of Packet Capture (Step 1 of 6)
9. 	Use this wizard to configure and run capture. The wizard will run one capture on each of the ingress and egress interfaces. After capturing you can save the captures to your PC for examination or replay in a packet analyzer. The wizard will guide you through the following tasks:
	Select an ingress interface. Select an egress interface. Set the buffer parameters. Run the captures. Save the captures to your PC (optional).
	< Back Next > Finish Cancel Help

3.0在新視窗中,提供用於擷取輸入流量的引數。

3.1選擇 inside 對於 Ingress Interface 並在提供的相應空間中提供要捕獲的資料包的源IP地址和目的IP地 址及其子網掩碼。

3.2選擇要由ASA捕獲的資料包型別(IP是此處選擇的資料包型別),如下所示:

Capture Wizard				
Packet Capture Wizard	Ingress Traffic Selecto	r (Step 2 of 6)		
A REAL PROPERTY.	Point of Ingress			
A State	Select interface:	inside 💌		
	Use backplane cho	annel		
A.		Ingress	_	
and the second	-			
		••••• inside		
	Packet Match Criteria -			
and the second	Select access list:	botnet-exclude +	Manage	
144	Specify packet pa	rameters		
	Source Host:	192.168.10.10	Source Network:	255.255.255.255 •
2440111111	Destination Host:	203.0.113.3	Destination Network:	255.255.255.255 •
Think	Protocol:	ip -		
1 AL				
				1
			<back next=""> Fini</back>	sh Cancel Help

3.3按一下 Next.

4.1選擇 outside 對於 Egress Interface 並在提供的相應空白處提供源IP地址和目的IP地址及其子網掩碼 。

If Network Address Translation (NAT) 在防火牆上執行,也考慮這一點。

Capture Wizard			-X-
Packet Capture Wizard Egress Traffic	Selector (Step 3 of 6)		
Point of Egres	5		
Select a	nterface: joutside 🗸 👻		
O Use bac	kplane channel		
A.		Egress	
Contraction of the second s			
		outside	•• I
Packet Match	Oriteria		
O Select a	access list: [botnet-exclude +]	Manage	
Specify	packet parameters		
Source	Host: 192.168.10.10	Source Network:	255.255.255.255 -
Destinal	tion Host: 203.0.113.3	Destination Network:	255.255.255.255 -
Protoco	k (p v]	
The state			
9.91			
	[< Back. Next > Finit	sh Cancel Help
L	L. L.		

4.2按一下 Next.

5.1輸入適當的 Packet Size 和 Buffer Size 各個空間中。進行捕獲需要此資料。

5.2檢查 Use circular buffer 框中,使用循環緩衝選項。循環緩衝區永遠不會滿。

當緩衝區達到最大容量時,將丟棄舊資料並繼續捕獲。

在此示例中,未使用循環緩衝區,因此未選中該覈取方塊。



5.3按一下 Next.

6.0此視窗顯示 Access-lists 必須在ASA上配置(以便捕獲所需的資料包)以及要捕獲的資料包型別 (在本示例中捕獲IP資料包)。

6.1按一下 Next.



7.按一下 Start 若要開始封包擷取,如下所示:

Capture Wizard	-		C.,	x	
Packet Capture Wizard	Run Captures (Step 6 of 6)				
- State of the	Click the Start button to begin capturing.				
0	Start	Stop	Get Capture Buffer		
	Ingress: inside		Launch Network Sniffer Application)	
C.A.					
	Egress: management		Launch Network Sniffer Application]	
	Sa	e captures	Clear Buffer on Device		
			< Back Next > Finish Cancel	Help	

資料包捕獲啟動後,嘗試從內部網路ping外部網路,以便在ASA捕獲緩衝區捕獲在源和目標IP地址 之間流經的資料包。

8.按一下 Get Capture Buffer 檢視ASA捕獲緩衝區捕獲的資料包。

🛍 Capture Wizard		×
Packet Capture Wizard	Run Captures (Step 6 of 6)	
e	Start Stop Get Capture Buffer Click the Start button to begin capturing. Launch Network Sniffer Application	
	Egress: outside Launch Network Sniffer Application	
	Save captures Clear Buffer on Device < Back Next > Finish Cancel Help)

在此視窗中顯示入口和出口流量的已捕獲資料包。

9.按一下 Save captures 儲存捕獲資訊。

Capture Wittard			-		-	~
Packet Capture Wizard	Run Captures (Step 6	of 6)				
- Statistics	Click the Start button to b	begin capturing.				
0		Start	Stop	Get Capture Buffer		
	Ingress	: inside		Launch Network Sniffer	Application	
Jal /	1:03:58:37.845262	192, 168, 10, 10 > 2	203.0.113.3; k	ono: echo request		
and the second	2:03:58:37.845903	203.0.113.3 > 19/	2.168.10.10: k	cmp: echo reply		
	3: 03:58:37.846941	192, 168, 10, 10 > 1	203.0.113.3: k	onp: echo request		
	4: 03:58:37.847520	203.0.113.3 > 19/	2.168.10.10: k	cmp: echo reply		121
	5: 03:58:37.848299	192.168.10.10 > 2	203.0.113.3: k	cmp: echo request		1
	6:03:58:37.848665	203.0.113.3 > 19/	2. 168. 10. 10; k	onp: echo reply		
	7:03:58:37.849443	192, 168, 10, 10 > 2	203.0.113.3; k	cmp: echo request		LUI,
State in he	8:03:58:37.849824	203.0.113.3 > 192	2.168.10.10: k	cmp: echo reply		
11	9:03:58:37.850618	192, 168, 10, 10 > 1	203.0.113.3; k	cmp: echo request		
	10: 03:58:37.850984	203.0.113.3 > 19	2.168.10.10:	icmpt echo reply		
	11:03:58:38.868302	192.168.10.10 >	203.0.113.3:1	icmp: echo request		
	12:03:58:38.868897	203.0.113.3 > 19	2.168.10.10	icmp: echo reply		*
TTHU	Egress	outside		Launch Network Sniffer	Application	
	1:03:58:17.845491	192, 168, 10, 10 > 1	203.0.113.3:4	trauper othe request		
- 13-	2:03:58:37.845873	203.0.113.3 > 19	2, 168, 10, 10; 6	cmp: echo regiv		6
000	3: 03:58:37.847139	192, 168, 10, 10 > 2	203.0.113.3: 4	cmp: echo request		
9.97 J	4:03:58:37.847490	203.0.113.3 > 19	2, 168, 10, 10; k	ono: echo reply		11
	5:03:58:37.848314	192, 168, 10, 10 > 2	203.0.113.3: 6	cmp: edho request		1
	6: 03:58:37.848634	203.0.113.3 > 19	2, 168, 10, 10; k	cmp: echo reply		
	7:03:58:37.849458	192, 168, 10, 10 > 1	203.0.113.3; k	cmp: edho request		
	8: 03:58:37.849794	203.0.113.3 > 19	2, 168, 10, 10; k	cmp: echo reply		
	9: 03:58:37.850648	192, 168, 10, 10 > 3	203.0.113.3; k	cmp: echo request		
	10: 03:58:37.850953	203.0.113.3 > 19	2, 168, 10, 10;	iono: echo reoly		
	11:03:58:38.868500	192.168.10.10 >	203.0.113.3	iono: echo request		
	12:03:58:38.868866	203.0.113.3 > 19	2.168.10.10:	icmp: echo reply		*
		Save cap	tures	Clear Buffer on Device		
				<back next=""></back>	Finish Cancel He	þ

10.1來自 Save captures 視窗中,選擇儲存捕獲緩衝區所需的格式。

10.2這是ASCII或PCAP。按一下格式名稱旁邊的單選按鈕。

10.3然後,按一下 Save ingress capture 或 Save egress capture 根據需要。

可以使用捕獲分析器開啟PCAP檔案,例如 Wireshark,並且它是首選方法。

🖆 Save Captures 🛛 🔀
ASCII PCAP Save the buffer in the specified format to the localhost.
Save egress capture
Close Help

11.1來自 Save capture file 視窗中,提供檔名和儲存捕獲檔案的位置。

11.2按一下 Save.

Save capture f	ile				? 🔀
Save in:	Capture date	٠	•	🗢 🗈 💣 🗊 •	,
My Recent Documents					
Desktop					
My Documents					
My Computer					
My Network Places	File name: Save as type:	ingress All Files (".")		•	Save Cancel

12.按一下 Finish.



這樣就完成了GUI資料包捕獲過程。

使用CLI配置資料包捕獲

完成以下步驟,以便使用CLI在ASA上配置資料包捕獲功能:

- 1. 使用正確的IP地址和安全級別配置網路圖所示的內部和外部介面。
- 2. 在特權執行模式下使用capture命令啟動資料包捕獲過程。在此配置示例中,定義了名為 capin的捕獲。將其繫結到inside介面,並使用match關鍵字指定僅捕獲與所關注流量匹配的資 料包:

ASA# capture capin interface inside match ip 192.168.10.10 255.255.255.255 203.0.113.3 255.255.255.255

 同樣,定義名為capout的捕獲。將其繫結到outside介面,並使用match關鍵字指定僅捕獲與所 關注流量匹配的資料包:

ASA# capture capout interface outside match ip 192.168.10.10 255.255.255.255 203.0.113.3 255.255.255.255

ASA現在開始捕獲介面之間的流量。要隨時停止捕獲,請輸入no capture命令,後跟捕獲名稱

以下是範例:

no capture capin interface inside no capture capout interface outside

ASA上的可用捕獲型別

本節介紹ASA上可用的各種捕獲型別。

• asa_dataplane — 捕獲在ASA背板與使用背板的模組(如ASA CX或IPS模組)之間傳遞的資料包 0

```
ASA# cap asa_dataplace interface asa_dataplane
ASA# show capture
```

capture asa_dataplace type raw-data interface asa_dataplane [Capturing - 0 bytes]

• asp-drop drop-code — 捕獲加速安全路徑丟棄的資料包。丟棄代碼指定加速安全路徑丟棄的流量 型別。

```
ASA# capture asp-drop type asp-drop acl-drop
ASA# show cap
ASA# show capture asp-drop
```

2 packets captured

```
1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2 packets shown
```

ASA# show capture asp-drop

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S 2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop) Flow is denied by configured rule 2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S 2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop) Flow is denied by configured rule 2 packets shown

• ethernet-type type — 選擇要捕獲的乙太網型別。支援的乙太網型別包括8021Q、ARP、IP、 IP6、LACP、PPPOED、PPPOES、RARP和VLAN。

以下範例顯示如何擷取ARP流量:

```
ASA# cap arp ethernet-type ?
```

802.10 <0-65535> Ethernet type arp ip ip6 pppoed pppoes rarp vlan cap arp ethernet-type arp interface inside ASA# show cap arp 22 packets captured 1: 05:32:52.119485 arp who-has 10.10.3.13 tell 10.10.3.12 arp who-has 192.168.10.123 tell 192.168.100.100 2: 05:32:52.481862 3: 05:32:52.481878 arp who-has 192.168.10.50 tell 192.168.100.10 4: 05:32:53.409723 arp who-has 10.106.44.135 tell 10.106.44.244 5: 05:32:53.772085 arp who-has 10.106.44.108 tell 10.106.44.248 6: 05:32:54.782429 arp who-has 10.106.44.135 tell 10.106.44.244 7: 05:32:54.784695 arp who-has 10.106.44.1 tell xx.xx.xx.xx: • real-time — 連續即時顯示捕獲的資料包。要終止即時資料包捕獲,請按Ctrl-C。要永久刪除捕獲 , 請使用此命令的no形式。

• 當您使用 cluster exec capture 指令。

ASA# cap capin interface inside real-time

Warning: using this option with a slow console connection may result in an excessive amount of non-displayed packets due to performance limitations.

Use ctrl-c to terminate real-time capture

• Trace — 以類似ASA Packet Tracer功能的方式跟蹤捕獲的資料包。

ASA#cap in interface Webserver trace match tcp any any eq 80

// Initiate Traffic

1: 07:11:54.670299 192.168.10.10.49498 > 198.51.100.88.80: S
2322784363:2322784363(0) win 8192
<mss 1460,nop,wscale 2,nop,nop,sackOK>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

MAC Access list

Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 0.0.0.0 0.0.0.0 outside Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group any in interface inside access-list any extended permit ip any4 any4 log Additional Information: Phase: 5 Type: NAT Subtype: Result: ALLOW Config: object network obj-10.0.0.0 nat (inside,outside) dynamic interface Additional Information: Dynamic translate 192.168.10.10/49498 to 203.0.113.2/49498 Phase: 6 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 8 Type: Subtype: Result: ALLOW Config: Additional Information: Phase: 9 Type: ESTABLISHED Subtype: Result: ALLOW Config: Additional Information: Phase: 10 Type: Subtype: Result: ALLOW Config: Additional Information:

Phase: 11 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 12 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 13 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 41134, packet dispatched to next module Phase: 14 Type: ROUTE-LOOKUP Subtype: output and adjacency Result: ALLOW Config: Additional Information: found next-hop 203.0.113.1 using egress ifc outside adjacency Active next-hop mac address 0007.7d54.1300 hits 3170

```
Result:
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

附註:在ASA 9.10+上,any關鍵字僅捕獲具有ipv4地址的資料包。any6關鍵字捕獲所有 ipv6定址流量。

以下是可使用封包擷取設定的進階設定。

請檢視命令參考指南,瞭解如何設定它們。

- ikev1/ikev2 僅捕獲Internet金鑰交換版本1(IKEv1)或IKEv2協定資訊。
- isakmp 捕獲VPN連線的網際網路安全關聯和金鑰管理協定(ISAKMP)流量。ISAKMP子系統無權訪問上層協定。捕獲是偽捕獲,將物理、IP和UDP層結合在一起以滿足PCAP分析器的要求。對等體地址從SA交換獲得並儲存在IP層中。

• tls-proxy — 從一個或多個介面上的傳輸層安全(TLS)代理捕獲已解密的入站和出站資料。

• webvpn — 捕獲特定WebVPN連線的WebVPN資料。

注意:啟用WebVPN捕獲時,它會影響安全裝置的效能。請確保在生成故障排除所需的捕獲 檔案後禁用捕獲。

預設值

以下是ASA系統預設值:

- 預設型別為raw-data。
- •預設緩衝區大小為512 KB。
- 預設乙太網型別為IP資料包。
- •預設資料包長度為1,518位元組。

檢視捕獲的資料包

在ASA上

要檢視捕獲的資料包,請輸入show capture命令,後跟捕獲名稱。本節提供捕獲緩衝區內容的 show命令輸出。其 show capture capin 命令顯示名為的捕獲緩衝區的內容 capin:

ASA# show cap capin

8 packets captured

1: 03:24:35.526812 192.168.10.10 > 203.0.113.3: icmp: echo request 2: 03:24:35.527224 203.0.113.3 > 192.168.10.10: icmp: echo reply 3: 03:24:35.528247 192.168.10.10 > 203.0.113.3: icmp: echo request 4: 03:24:35.528582 203.0.113.3 > 192.168.10.10: icmp: echo reply 5: 03:24:35.529345 192.168.10.10 > 203.0.113.3: icmp: echo request 6: 03:24:35.529681 203.0.113.3 > 192.168.10.10: icmp: echo reply 7: 03:24:57.440162 192.168.10.10 > 203.0.113.3: icmp: echo request 8: 03:24:57.440757 203.0.113.3 > 192.168.10.10: icmp: echo reply

其 show capture capout 命令顯示名為的捕獲緩衝區的內容 capout:

ASA# show cap capout

8 packets captured

```
1: 03:24:35.526843 192.168.10.10 > 203.0.113.3: icmp: echo request

2: 03:24:35.527179 203.0.113.3 > 192.168.10.10: icmp: echo reply

3: 03:24:35.528262 192.168.10.10 > 203.0.113.3: icmp: echo request

4: 03:24:35.528567 203.0.113.3 > 192.168.10.10: icmp: echo reply

5: 03:24:35.529361 192.168.10.10 > 203.0.113.3: icmp: echo request

6: 03:24:35.529666 203.0.113.3 > 192.168.10.10: icmp: echo reply

7: 03:24:47.014098 203.0.113.3 > 203.0.113.2: icmp: echo request

8: 03:24:47.014510 203.0.113.2 > 203.0.113.3: icmp: echo reply
```

從ASA下載以進行離線分析

以下幾種方法可以離線下載資料包捕獲進行分析:

1. 導航至 https://<ip_of_asa>/admin/capture/<capture_name>/pcap在任何瀏覽器上。

提示:如果您不考慮 pcap 關鍵字,則只有等效於 show capture 提供了命令輸出。

1. 輸入copy capture命令和您的首選檔案傳輸協定以下載捕獲:

copy /pcap capture:<capture-name> tftp://<server-ip-address>

提示:對資料包捕獲的使用問題進行故障排除時,思科建議您下載捕獲以進行離線分析。

清除捕獲

若要清除擷取緩衝區,請輸入 clear capture 指令:

ASA# **show capture** capture capin type raw-data interface inside [Capturing - 8190 bytes] match icmp any any capture capout type raw-data interface outside [Capturing - 11440 bytes] match icmp any any

ASA# clear cap capin ASA# clear cap capout

ASA# **show capture** capture capin type raw-data interface inside [Capturing - 0 bytes] match icmp any any capture capout type raw-data interface outside [Capturing - 0 bytes] match icmp any any **輸入 clear capture /all 命令清除所有擷取的緩衝區**:

ASA# clear capture /all

停止捕獲

在ASA上停止捕獲的唯一方法是使用以下命令完全禁用捕獲:

no capture <capture-name>

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。