

安全防火牆FTD — 縮放電話音訊阻止清單；由於舊的VDB

目錄

問題

使用者遇到呼叫連線但音訊丟失的縮放電話呼叫的音訊問題。FTD正在從Zoom IP範圍中丟棄UDP媒體資料包，將其顯示為資料包捕獲和ASP丟棄計數器中的Snort列出的阻塞。

具體症狀包括：

- 防火牆正在運行Cisco Vulnerability Database(VDB)427版或更低版本。
- 防火牆包含一個訪問規則，該規則必須根據Firepower資料庫提供的預設Zoom/RTP應用ID允許縮放流量。根據appid.cisco.com，規則必須允許所有這些埠通過Zoom AppID:
 - UserZoom(6243):80,443/tcp
 - 縮放下載(4628):80,443/tcp
 - 縮放上傳(4627):80,443/tcp
 - 縮放會議(4629):80/tcp
 - RTP音訊(2475):5004/udp
 - SIP(426):5060/udp
- 但是，Packet Tracer輸出顯示，由於阻止清單原因「被防火牆前處理器阻止或列入黑名單」，流量被丟棄。

<#root>

Phase: 17
Type: SNORT
Subtype: firewall

Result: DROP

Elapsed time: 345716 ns
Config:

Network 0, Inspection 0, Detection 4, Rule ID 268434438

Additional Information:

Starting rule matching, zone 3 -> 3, geo 840 -> 840, vlan 0, src sgt: 0, src sgt type: unknown, ds

Matched rule ids 268434438 - Block

Result:

input-interface: Outside(vrfid:0)

input-status: up

input-line-status: up

output-interface: Outside(vrfid:0)

output-status: up

output-line-status: up

Action: drop

Time Taken: 640578 ns

Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame

- 資料包捕獲show drops with reason: 「snort-blacklist」。

<#root>

40: 22:52:36.383692 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

141: 22:52:36.383723 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

142: 22:52:36.385188 206.247.118.57.60030 > 10.X.X.1.9178: udp 44

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

- 在system support trace輸出中，由於應用程式標識處於掛起狀態，因此流量在規則匹配期間被延遲。但是，流量被錯誤識別並被阻止列出。IP地址是根據Zoom文章[Zoom network firewall or proxy server settings要求訪問的Zoom公共IP](#)。

<#root>

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

pending rule order 12, 'allow-outbound', AppID

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

Deferring trust until a rule is matched

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

match rule order 28, 'Default Block', action Block

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 MidRecovery data sent for rule id: 26843

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Matched a rule, stop deferring trust

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Generating an SOF event with rule_id = 2

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

deny action

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Deleting Firewall session flags=0x20, 1c

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Packet 17168248: UDP, 04/14-14:44:53.110

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Firewall: starting rule matching, zone 1

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Firewall: block rule, 'Default Block', force_block

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

AppID: service: (-1), client: (0), payload: (0), misc: (0)

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Stream: pending block, drop

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Policies: Network 0, Inspection 0, Detect

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Verdict: blacklist

- 當縮放IP嘗試響應時，系統支援跟蹤指示「RTP客戶端候選返回錯誤 — 無效(-11)」和「第三方返回未知(0)」消息。

<#root>

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1 New AppId session

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

3rd party returned unknown (0)

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

RTP client candidate returned error-invalid (-11)

10.X.X.1 9824 -> 206.247.118.55 54808 17 AS=0 ID=2 GR=1-1 app event changes: created

- FTD show asp drop命令顯示阻止清單丟棄的快速增量。

<#root>

Frame drop:

-----ABBREVIATED-----

Blocked or blacklisted by the firewall preprocessor (firewall)	11224
Blocked or blacklisted by the stream preprocessor (stream)	2354
Fragment reassembly failed (fragment-reassembly-failed)	3
Packet is blacklisted by snort (snort-blacklist)	27173
Packet is blocked as requested by snort (snort-block)	42

環境

- 由FMC管理的Cisco Firepower FTD版本7.7.11
- 漏洞資料庫(VDB)版本427或更低版本
- Snort版本3.3.5.1100-66
- 主要影響Zoom IP子網170.114.0.0/16和206.247.0.0/16的流量，但可能包括其他Zoom IP

解析

思科錯誤ID CSCwu22106解決方法 — 預過濾器規則實施

1:為縮放流量建立預過濾器規則。

導覽至Policies > Access Control > Prefilter，然後使用以下配置建立新規則：

- 規則名稱：縮放預濾器
- Action:快速路徑
- 源區域：輸入介面

- 目標區域：輸出介面
- 來源位址:任意
- 源埠：任意
- 目的地位址:縮放IP範圍(170.114.0.0/16、206.247.0.0/16)和在[Zoom network firewall](#)或[Proxy server settings](#)中說明的任何其他設定。
- 目的地連線埠：UDP 10000-64000

2:備用訪問控制規則配置

如果不首選預過濾，請通過刪除縮放應用程式識別符號並使用顯式IP和埠匹配來修改現有的訪問控制策略規則：

- 規則名稱：Zoom-Allow
- Action:允許
- 源區域：輸入介面
- 目標區域：輸出介面
- 來源位址:任意
- 源埠：任意
- 目的地位址:縮放IP範圍(170.114.0.0/16、206.247.0.0/16)和在[Zoom network firewall](#)或[Proxy server settings](#)中說明的任何其他設定。
- 目的地連線埠：UDP / 「Zoom-Phone-Ports」(範圍10000 64000)
- 日誌記錄：(可選，用於監控允許的流量)

3:將組態變更部署到FTD裝置，並驗證是否已還原雙向音訊功能。

- 監視ASP刪除計數器以確認阻止清單已停止：

```
device# show asp drop
```

- 檢查資料包捕獲，確保雙向流量成功：

```
device# show capture
```

4:缺陷Cisco錯誤ID CSCwu22106在Cisco Vulnerability Database(VDB)版本428的發行版中已解決。Firepower裝置必須運行最新的VDB版本以避免此缺陷的影響。同樣，VDB版本395中解決了相關缺陷Cisco Bug ID CSCwn80786。

原因

漏洞資料庫(VDB)版本427中的Cisco安全防火牆應用識別簽名存在缺陷，導致Zoom Phone媒體流量被錯誤分類，隨後被Snort檢查引擎阻塞。此行為在Cisco錯誤ID CSCwu22106和相關缺陷Cisco錯誤ID CSCwn80786下跟蹤，該缺陷記錄了使用應用程式ID時對Zoom IP地址和媒體流的錯誤處理。

相關內容

- [縮放網路防火牆或代理伺服器設定](#)
- [快速路徑預過濾的最佳實踐](#)
- [Cisco錯誤ID CSCwu22106 — 在VDB 427中處理IP地址縮放不正確](#)
- [思科錯誤ID CSCwn80786 - Zoom應用檢測器未檢測到用於縮放電話的網路](#)
- [思科技術支援與下載](#)

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）。