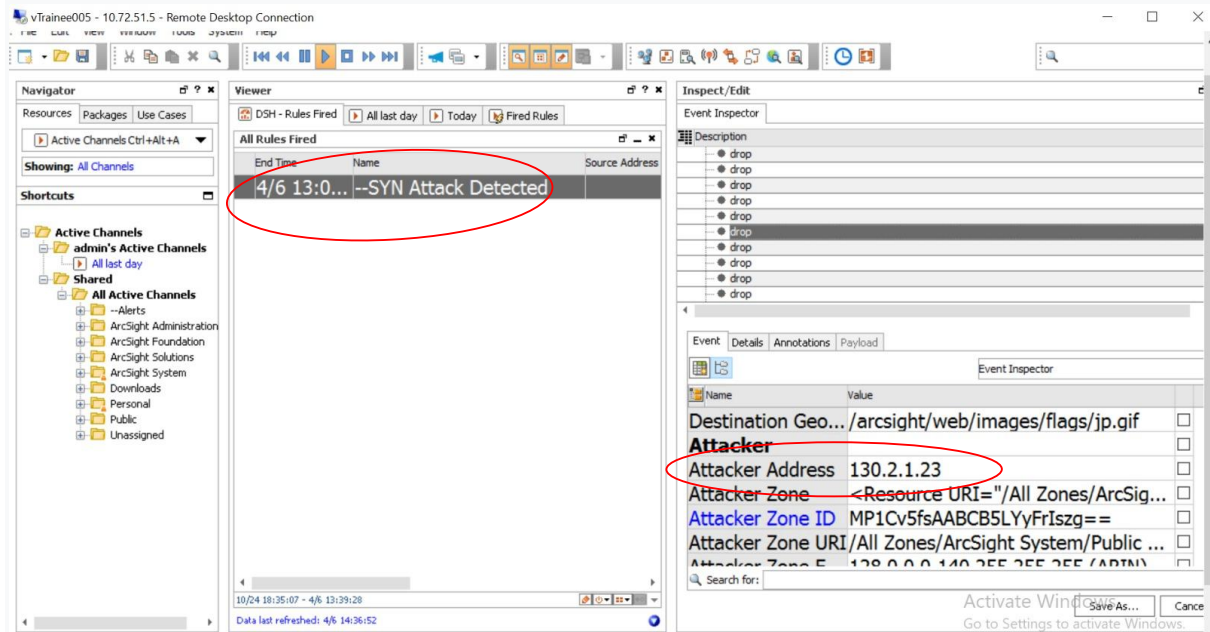
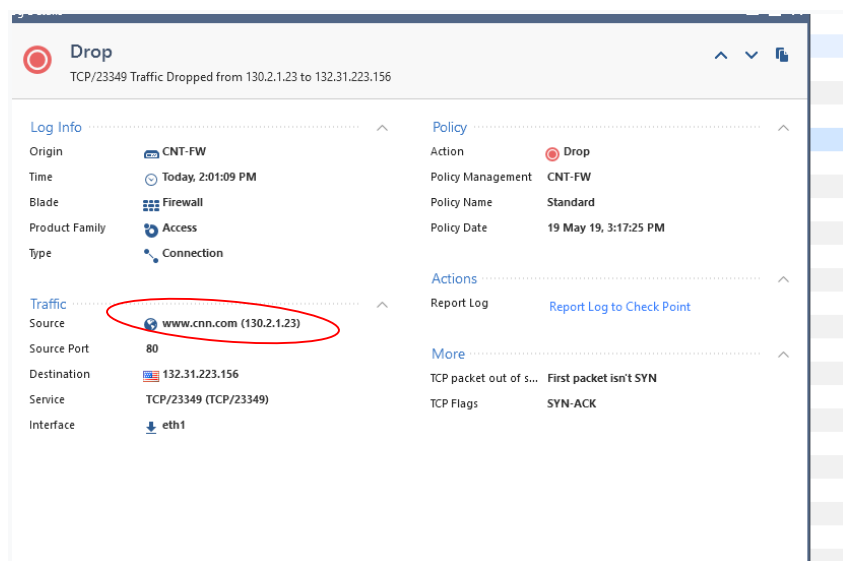


ב-4/6 בשעה 13:07:33 קיבלנו התרעה מי 192.168.66.1 לגבי SYN Attack--מזוהה.

SYN Attack - פועל על ידי יצירת חיבור חצי פתוח עם מארח. השרת המותקף, המקבל חבילת SYN לסנכרון דרך יציאה פתוחה, אמור לקבל ACK בתגובה. אבל במהלך ההתקפה, זה לא קורה, וכתוצאה מכך חיבור חצי פתוח. פעולות אלו מציפות את התור של השרת, ומגבילות משתמשים חדשים מליצור חיבור.



אנחנו רואים גם את כתובת ה-IP של התוקף 130.2.1.23  
כתובת זו שייכת לדומיין [www.cnn.com](http://www.cnn.com)



אנו רואים שברשת הפנימית 172.16.100.23 ip ויש לנו nat שמשנה את הכתובת ל-130.2.1.23 ושני ה-ip הללו שווים ל-[www.cnn.com](http://www.cnn.com) וזה אחד השרתים שלנו

רואים גם הרבה בקשות מי **www.cnn.com** למקומות שונים וכל הבקשות האלה עוברות בשנייה אחת ובכל פעם החיבור לא עובר תקין (drop)

vTraine005 - 10.72.51.5 - Remote Desktop Connection

Queries | All Time | Log File: Latest Log File | Enter search query (Ctrl+F)

Showing first 250 results (3.2 sec.) out of at least 250 results

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 2:03:43 PM	CNT-DMZ-FW	71.246.227.209		www.cnn.co...	http (TCP/80)	27	Internet_To_DM...	Standard	http Traffic Accepted...
Today, 2:03:54 PM	CNT-FW	174.94.14.80		www.cnn.co...	TCP/24604 (TCP/24604)			Standard	TCP/24604 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	80.219.224.161		www.cnn.co...	TCP/21748 (TCP/21748)			Standard	TCP/21748 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	22.99.16.226		www.cnn.co...	TCP/14033 (TCP/14033)			Standard	TCP/14033 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	57.19.100.125		www.cnn.co...	TCP/12420 (TCP/12420)			Standard	TCP/12420 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	122.26.146.22		www.cnn.co...	TCP/16545 (TCP/16545)			Standard	TCP/16545 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	132.31.223.156		www.cnn.co...	TCP/13037 (TCP/13037)			Standard	TCP/13037 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	223.181.92.177		www.cnn.co...	TCP/10424 (TCP/10424)			Standard	TCP/10424 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	221.20.96.162		www.cnn.co...	TCP/28251 (TCP/28251)			Standard	TCP/28251 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	222.215.134.86		www.cnn.co...	TCP/32355 (TCP/32355)			Standard	TCP/32355 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	36.68.100.131		www.cnn.co...	TCP/23384 (TCP/23384)			Standard	TCP/23384 Traffic Dro...
Today, 2:03:54 PM	CNT-FW	57.19.100.125		www.cnn.co...	TCP/30804 (TCP/30804)			Standard	TCP/30804 Traffic Dro...

URLs | Files | Current Connection | Enter search query (Ctrl+F)

Found 0 results (98.9 sec.)

No matches found for your search

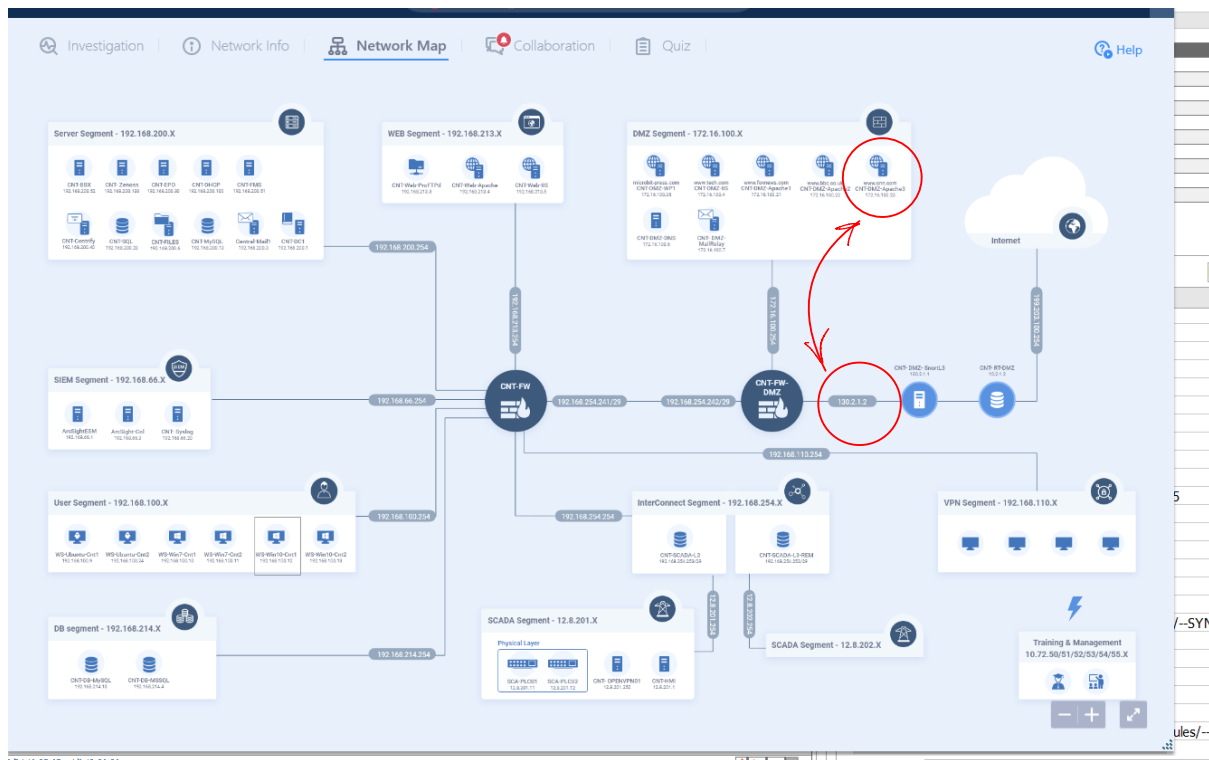
תמיד יש שלושה שלבים:

SYN - השולח שולח syn, מודיע שהוא רוצה להתחיל את ההעברה

SYN-ACK - המקלט משיב עם syn-ack אם הוא מוכן ליצור חיבור

ACK - השולח מאשר שקיבל את ה-syn-ack

אבל זה לא קורה אצלנו, ומכל האמור לעיל עולה שזו בעצם התקפת SYN



כיצד להתגונן מפני התקפות SYN:

- (1) אתה צריך לגשת לשרת
- (2) לקבל מידע על ההתקפה הזו
- (3) אם אנו משתמשים בfirewall לתעבורה נכנסת, עליך להשבית את כל הכללים מלבד חסימה
- (4) יש לחדש drivers בזמן, לפזר טיפול בהפסקות למעבדים שונים, להפעיל syn-cookies ולבטל את syn-cache