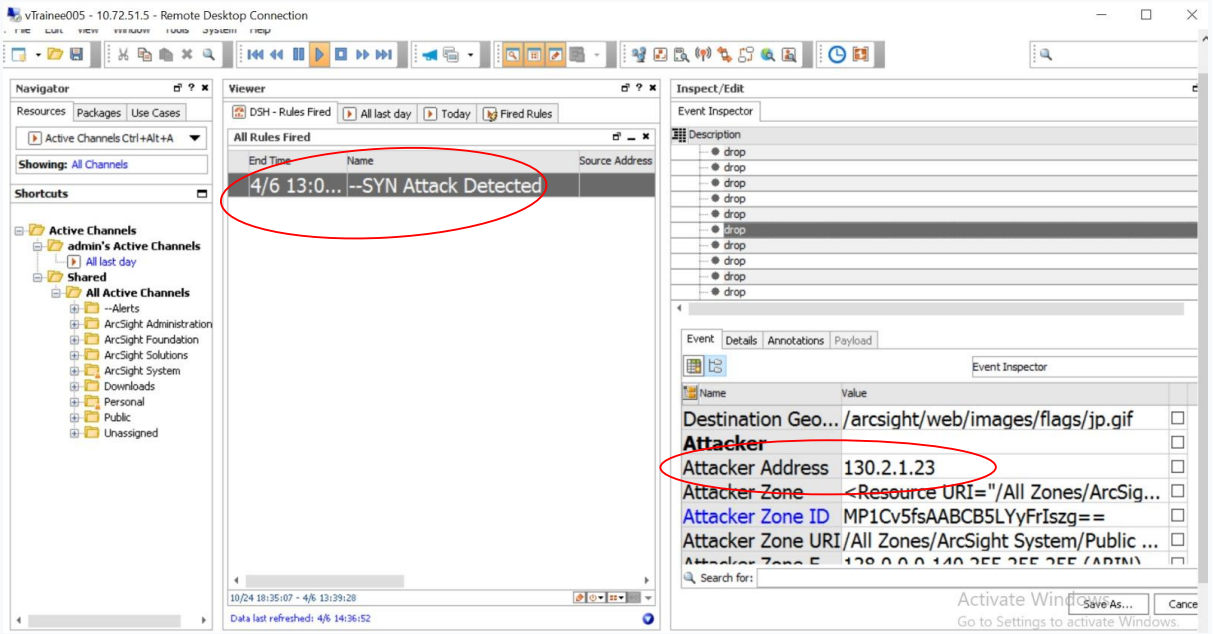
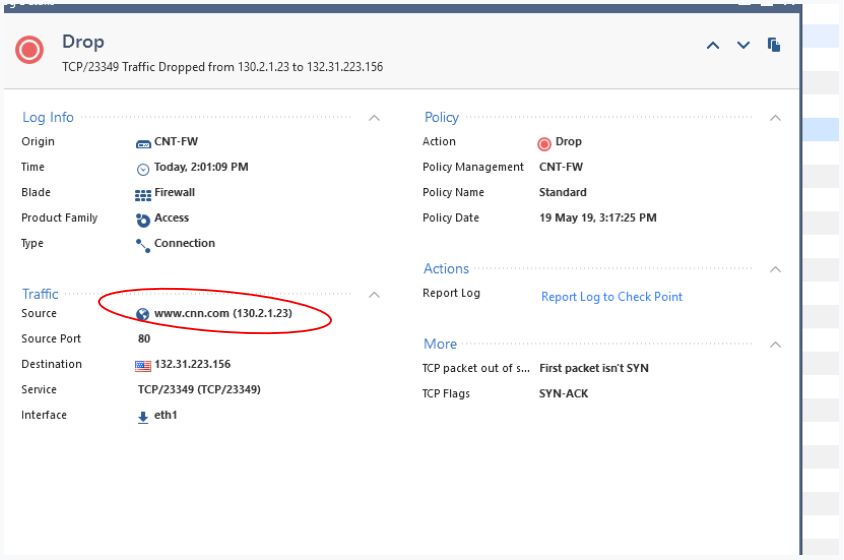
ב-4/6 בשעה 13:07:33 קיבלנו התרעה מי 192.168.66.1 לגבי --SYN Attack מזוהה.

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.

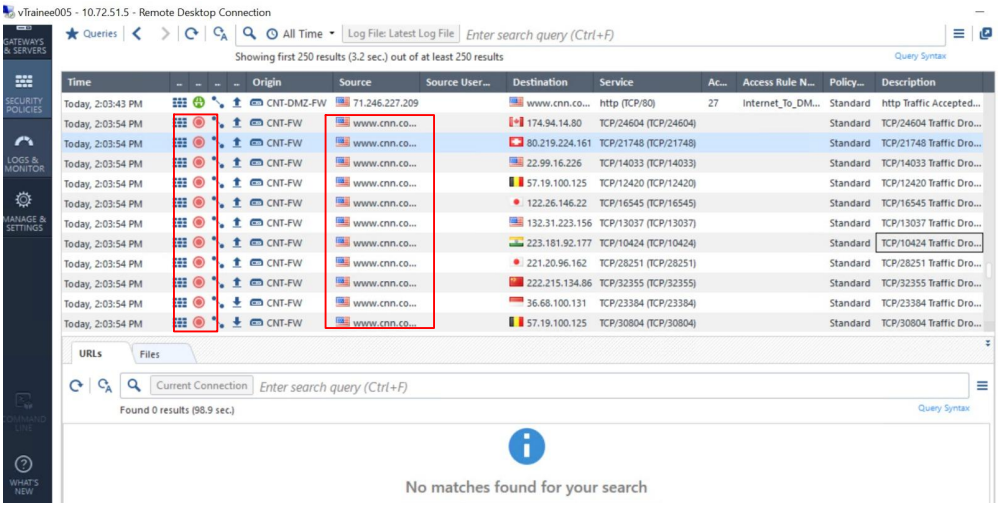


אנחנו רואים גם את כתובת ה-IP של התוקף 130.2.1.23 כתובת זו שייכת לדומיין www.cnn.com



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 ו זה 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)



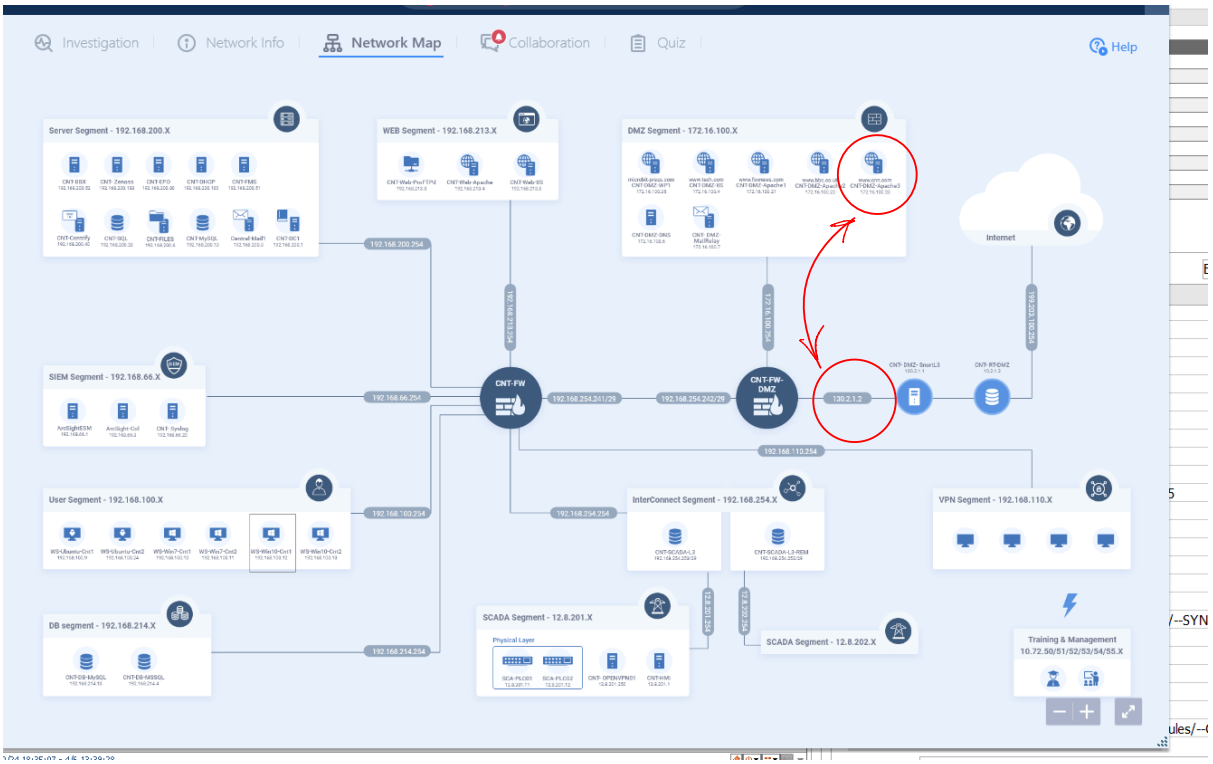
תמיד יש שלושה שלבים:

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