Bypassing Next Generation firewall

By: Ahmad Abdelnasser Soliman

abdelnassersoliman0@gmail.com

Index Of Content :

- فالاول كدا عاوزين نعرف ايه هو ال NGFW وايه هي وظيفته ... ؟؟

- ال Fire wall عموما بيقف زي حاجز بين الانترنت ال هو ال WAN وبين شبكتك انت ال هي ال LAN وليه شويه Rules انت بتحددها وبيقوم مطبقها على ال Traffic اللى جي من الانترنت وعاوز يدخل الشبكه عندك لو لقاه تمام ومطابق لل Rules ال انت حططهاله بيقوم مدخلك لقاك مش تمام وال traffic بتاعك في حاجه مشبوهه أو مش مسمحولك تدخل اساسا وال Network Administrator مانع اي حد يجي من برا يدخل لل Network جوا وطبعا كل دا بال Rules اللى بيكون محددها لل Fire wall فهتلاقيه يمنعك من الدخول ....

- ال Fire Wall دا هو الجيل الجديد من ال Fire walls وهو متقدم فتقنيات الحمايه عن ال Fire Walls التقليديه...

فأنه بيعمل Deep inspection لل Packets اللى بتعدي فال Network ويقدر يتعرف عليها اذا كانت بتحتوي على Malware مثلا ولا لاء ...

- كمان بيضم معاه على ال Fire wall العادي ال IPS وال IDS ال هما ال Intrusion detection system وال Intrusion prevention system ودي تقنيات بتقدر تعمل Detect لل Software malicious وتمنعها من الدخول لل Network عندك واصابه الاجهزة اللى فيها ... فدا بيعزز من قوه ال NGFW عن غيره .

- عشان ننجز ال Fire wall بتتلخص في خمس حاجات وهم كالاتي :

- ال Access Control وال threat prevention وال Traffic Filtering وال Logging & monitoring وال NAT ...

- ال Access control بينظم حركه المرور فالشبكه طبقا لل Rules ال انت برمجته عليها بيسمح مين يدخل ومين لاء ...

- ال Threat preventation بيمنع التهديدات ال جايه من ال WAN زي الهجمات ال بينفذوها ال Attackers عن طريق ال Malwares اللى بيبعتوها فال Packet ال داخله عندك ال Network ...

- ال Traffic filtering بيعمل Filter لل Traffic اللى جي من برا وداخل عندك ال Network ويشوف هل مسموحله ولالاء وهل يعديه ولا يعمله Block طبقا لمعايير زي ال IP بتاع ال Source وال Destination وكمان ال Port Numbers وكمان ال Protocols ال بيستخدمه ...

- فمثلا انت محدد rule لل Fire wall انه ميسمحش لاي حد جاي من برا الانترنت من ال WAN عاوز يدخل من Port 21 الخاص بال FTP لل Network بتعتك فهتلاقي ال Fire wall بيمنع اي حد عاوز يدخل لل Network من خلال ال Port دا ... هتلاقيه بيطلعلك لو انت شغال بال Nmap ان ال Port دا حالته Filter يعني فيه Fire wall منعك من الوصول ودا هنشوف ازاي نتخطاه من خلال الشرح دا باءذن الله ... طب لو ال Network Administrator عامل تخصيص لكام IP خاصين ب Clients معينه انهم يدخلوا من خلال نفس ال Port اللى اتمنعت منه .. كل دا هتلاقيه بيتم برضه من خلال Rule معينه بيضفها لل Fire wall ....

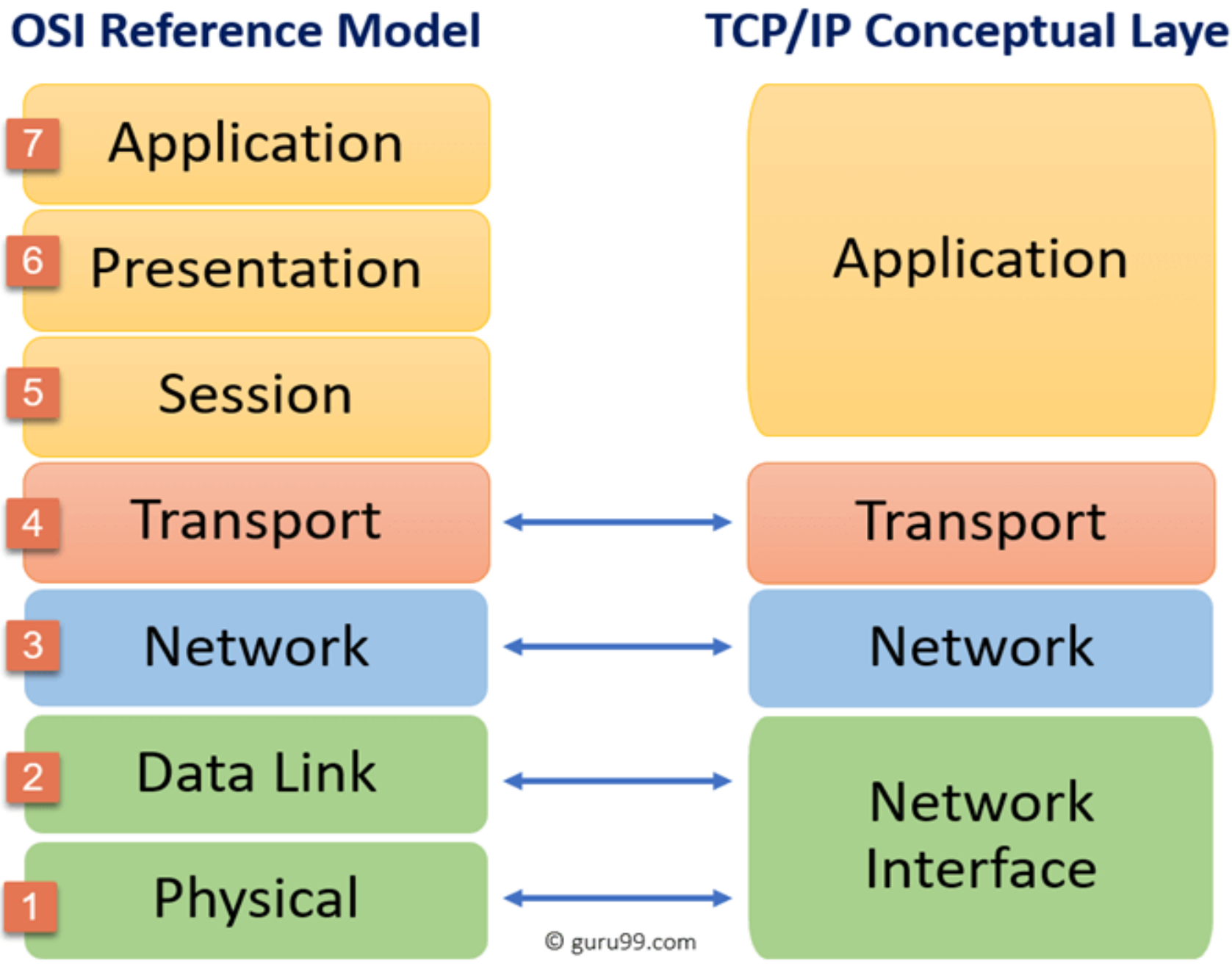
- ال Logging & monitoring دا المسؤول عن انه يحتفظلك بال Events اللى بتم فال Network فال registers زي مثلا اني كان فيه IP جاي من ال WAN وعاوز يدخل ال Network عندك لكنه فشل أو اتعمله Drop أو Block ...

ـ دا كله بيتعمله Logging فال Registers عشان اما تحب ترجعلها اي وقت ف Incident مثلا تعمل Investigation تلاقيها ودا اللى بيعمله ال Fire wall ... وكمان بيقدر يعمل Monitoring لل traffic اللى ماشي فيه زي موضحنا فوق ويحلله ويطلعلك المشبوه منه اللى عمله حظر وهكذا ...

ـ عندنا بعد كدا تقنيه ال NAT وهي ال Network Address Translation ودي وظيفتها انها بتشتغل مترجم ... تترجم ال IP الداخلي بتاع شبكتك ل IP خارجي لما تيجي تطلع للانترنت فمثلا انت موجود جوا ب IP ال 192.168.1.2 لما تيجي تطلع برا دي بتقوم محولاك ل IP خارجي مثلا زي 41.234.148.1 ال بيعمل العمليه دي هي ال NAT والعكس صحيح لو انت جي من ال WAN وداخل لل LAN ...

ـ فدا اللي بيعمله ال Fire wall عاوز تطلع لل WAN بيقوم واخد ال IP بتاعك ومحولك ل IP خارجي تستخدمه فقط وانت عال Internet برا ولما ترجع تاني لل LAN بيقوم مديك ال IP الداخلى بتاعك ال تستخدمه فال LAN ودا بيساعد فالحمايه عشان بيخفي ال IP الداخلي بتاع ال User .

ـ محتاجك الاول تكون عارف ال OSI Model وبتكون شغاله ازاي وانا هتكلم عن ال Layer اللى محتاجها فالشرح بتاعي وهي ال Application layer ال هي رقم 7 فال OSI model ورقم 4 فال TCP/IP model .



ـ لو جينا نبص على طريقه شغل ال **NGFW** هتلاقيها بتعتمد ف شغلها على حاجه مهمه وهي التضليل ... بمعنى عندك **Rule** جوا ال **Fire Wall** بتنص على ان مجموعه معينه من ال **IP** مسموحلها تستخدم ال **Ports 80,443** بتوع ال **Http** وال **Https** ال هما فالمعتاد بتستخدمهم عشان تبقا متصل بال **WAN** وال شغالين فالطبقه بتعتنا وهي ال **Application Layer** ...

ـ لو جيت انا ك **Attacker** عملت **Scan** بال **Nmap** على ال **Ports** المفتوحه عند ال**target** هتلاقي ان ال **Ports** مفتوحه فأنت تفرح وتقول ال **Fire Wall** مش شغال كويس لانه المفروض يديني ان ال **Ports** دي مقفوله ولكنه بيضللك لانك لو جيت تعمل **Connect** بال **Ports** دي هتلاقي مش هتعرف لانه فالحقيقه سايبها تظهرلك فال **Scan** انما لو جيت تستخدمها هتلاقي مش مسموحلك لانك مش من ضمن الناس ال مسموحلها فال **Rules** انها تستخدم ال **Ports** دي ...

ـ فالخلاصه ان ال NGFW ذكي شويه عن ال Fire walls التقليديه لأنه بيديك انطباع ان ال Ports مفتوحه لما يجي اي حد يعمل عليها Scan ب Tool زي ال Nmap انما فالواقع هو جواه Rules بتحدد مين يستخدم ال Ports دي ومين مش مسموحله وبالتالى اي Connect بال Ports دي غير اللى موجود فال rule الخاصه بيه بيعمل لل IP الخاص بيه Block .

ـ ناخد مثال مثلا على سلوك شغل ال NGFW ف Cisco هتلاقي عندنا Cisco fire power threat defense ال هو FTD ودا عباره عن كولكشن بين ال Fire wall واداه او محرك ال Snort اللى بيعمل Deep Investigation فال Packets ويطلع ال malicious منها او المشبوه وكل دا بال Rules ال انت بتحددها لل tool وكل دا فجهاز واحد وهو ال FTD ... حاجه صغيره عاوزك تفهمها فال Snort وهو انه علشان ال Snort يقدر يحدد الاتصال اللى طالع من الاجهزة زي مثلا انه FTP خاص بال Data Transfer أو Http خاص بال Web لازم يبص أو يعمل تفتيش على شويه Packets عشان يتأكد من الاتصال وفالمعتاد بيكون عددهم من 3 to 10 packets ودا بيختلف حسب نوع الاتصال ال انت بتنفذه ... خلال مال Snort بيعمل تفتيش عال packets عشان يعرف يحدد نوع الاتصال بتلاقي بعض من ال Packets الاخري بتعدي عادي من غير مال Snort يكون حدد ايه هو الاتصال ال انت عاوزه ودا عادي بيبقا مقصود من نظام ال Snort ذات نفسه ...

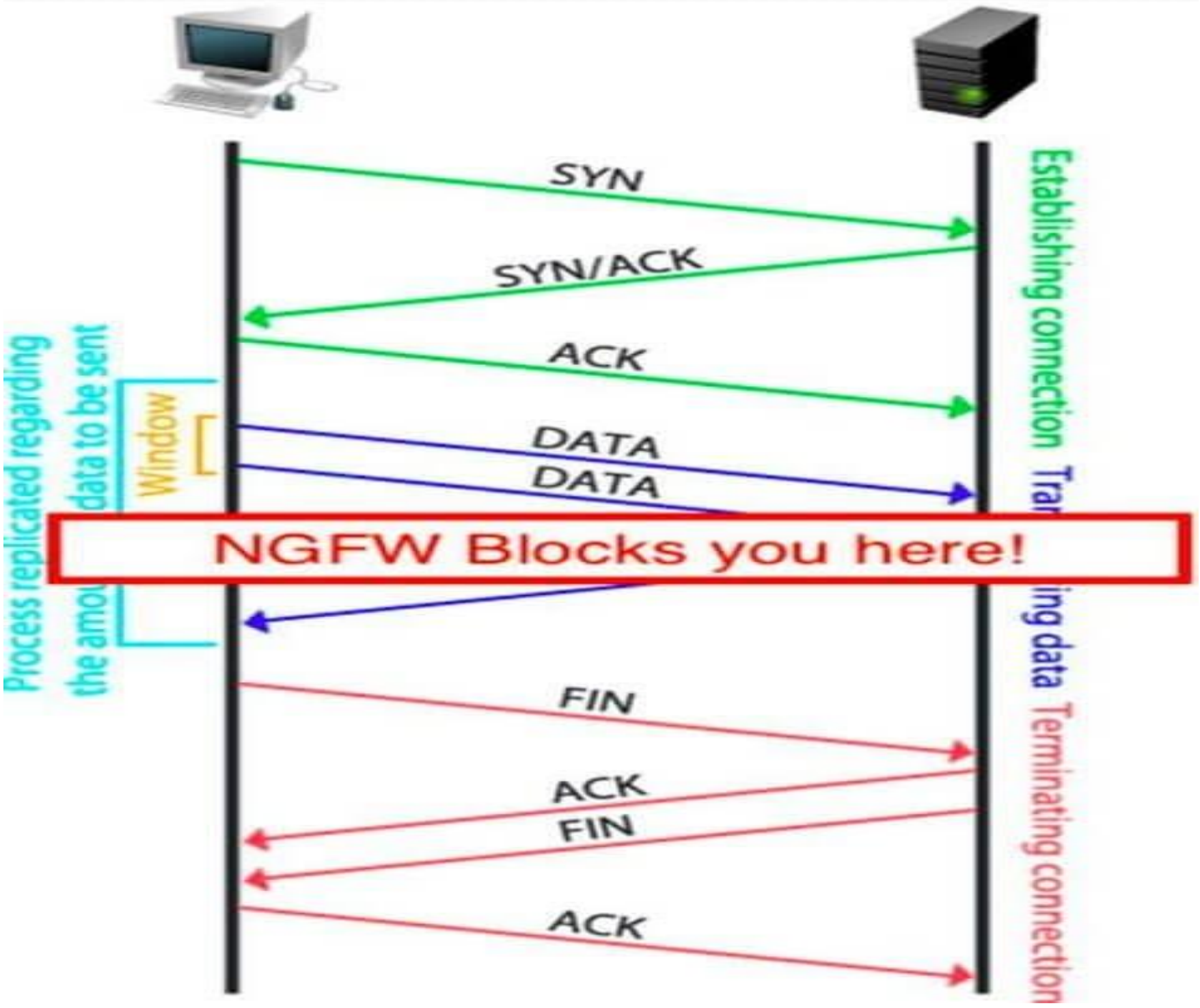
ـ بس خد بالك شويه ال Packets اللى فلتت من ال Snort دي بتفضل تحت عين ال Fire wall شايفها وبيراقبها قد تكون بتحمل حاجه malicious او مشبوهه ...

- ودا بيتم من خلال ال Setting في ال Fire wall ال هي Access policy ومنها ل Advanced ومنها ل Intrusion policy used before access control rule is determined

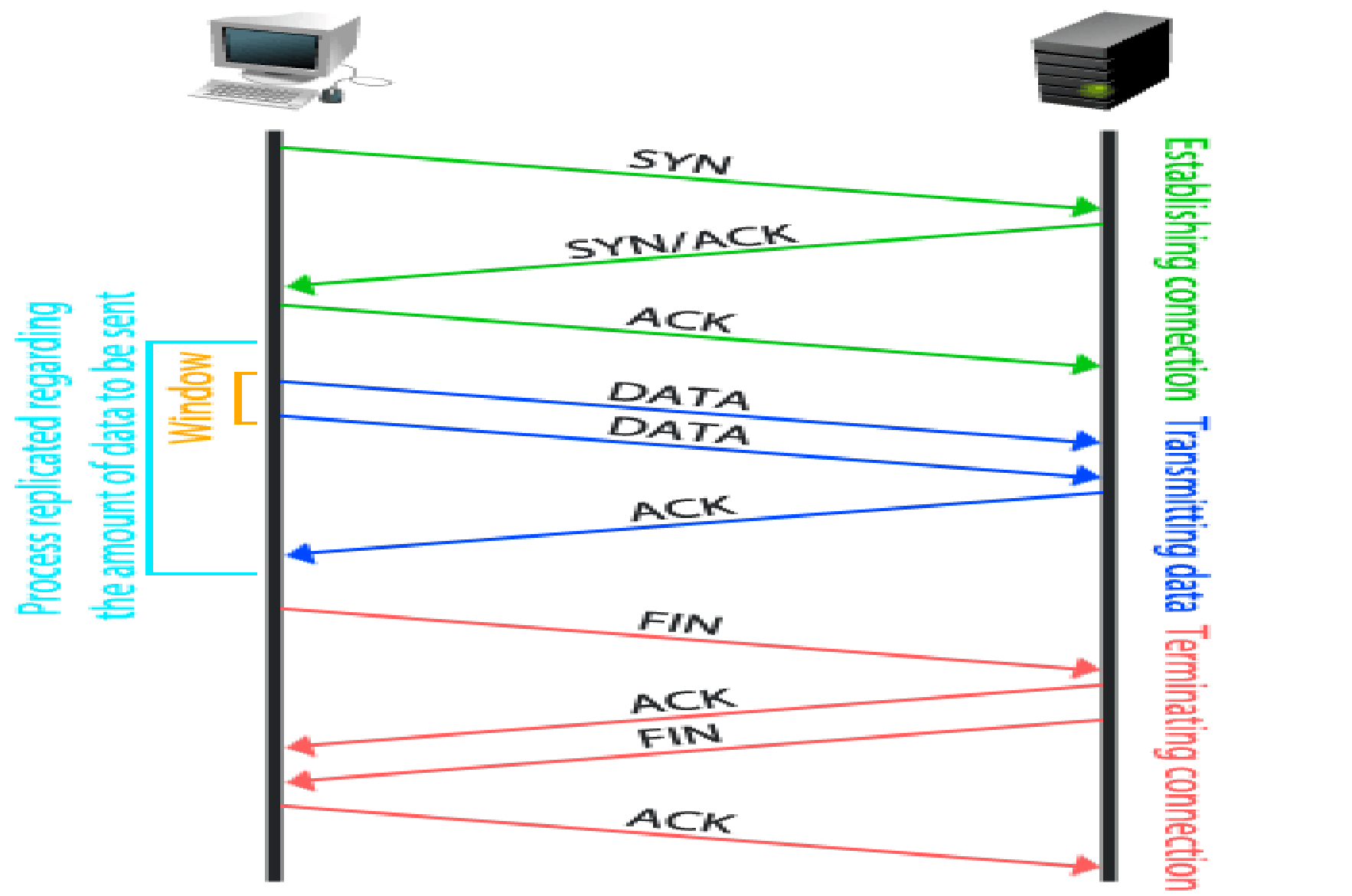
- بكدا بتكون فعلت الخاصيه دي من ال Fire wall بحيث اي حاجه تفلت من ال Snort يفضل ال Fire wall يراقبها لحد ميشوف هي تمام ولا فيها حاجه مشبوهه وبعد كدا بيطبق ال Rules بتعته عليها ... يعني اللى بياخد القرار النهاءي هو ال Fire wall اذا كان ال Packets دي تعدي ولا لاء ...

- عشان ننجز النقطه ال فاتت عندك ال Snort بيعمل حاجتين وهما انه بيعمل investigation لل packets ودي حوالي من 3 to 10 packets وبعد كدا بيسمح لبعض ال packets انها شويه تكمل طريقها لل target بتاعها سواء كان pc او server وال packets اللى عدت دي بتكون تحت عين ال rule ال قلنا عليها فال Fire wall ال بتراقب ال packets وتشوف فيها threat ولا لاء ...

- خد بالك حتى لو ال Connection باين انه بدء مع ال target ممكن ال fire wall يقفله بعد كدا لانه هو اللى بياخد القرار النهاءي بعد اما يتأكد من خلال ال policies’ ال فيه ان كل حاجه بتوافقها ... ومعنى ذلك ان مش كل connection يباللك انه مفتوح مع ال target تصدق عادي لان ال NGFW بيوقفها بعدين عشان يحللها ويشوفها واذا كانت clean بيعديها غير كدا بيعملها Drop .



عشان تبقا معايا لازم تكون فاهم ال TCP Connection بيحصل ازاي

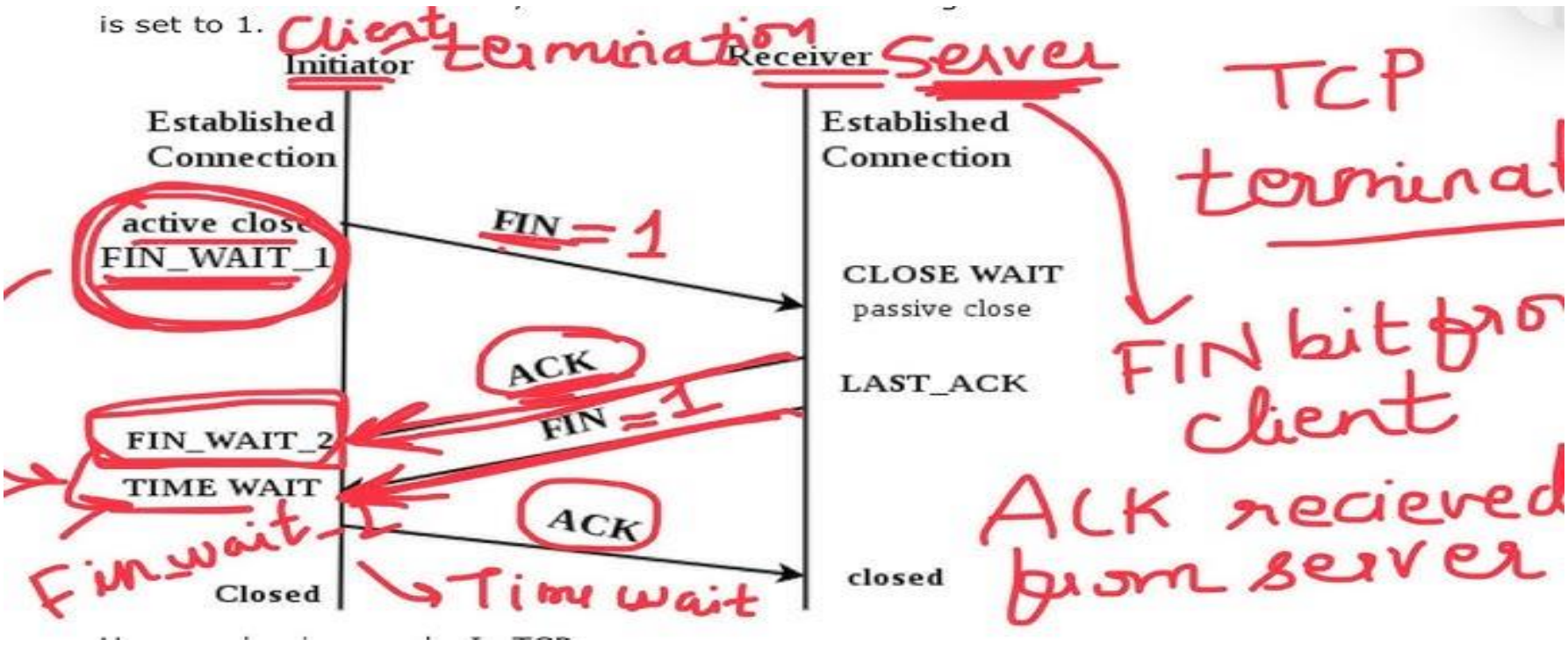


- ال TCP Connection بأختصار هو انك الجهاز ال عاوز يبدء الاتصال بيبعت Syn لل Destination ال عاوز يتصل بيه وبيقوله انا عاوز اتصل بيك ال هو (Syn) والخطوه اللى بعدها ان ال Destination اللى هو هنا ال PC او ال Server لو جاهز للاتصال معاك بيرد عليك بال (Syn-ack) يعني تمام انا موافق ابدء اتصال معاك ... بعد كدا ال Source بيبعتله ال Ack ودا كدا معناه ان ال Connection حصل بشكل كامل وتمام وبكدا يقدروا الجهازين يبعتوا Data لبعض عشان نشأ مبينهم Connection .

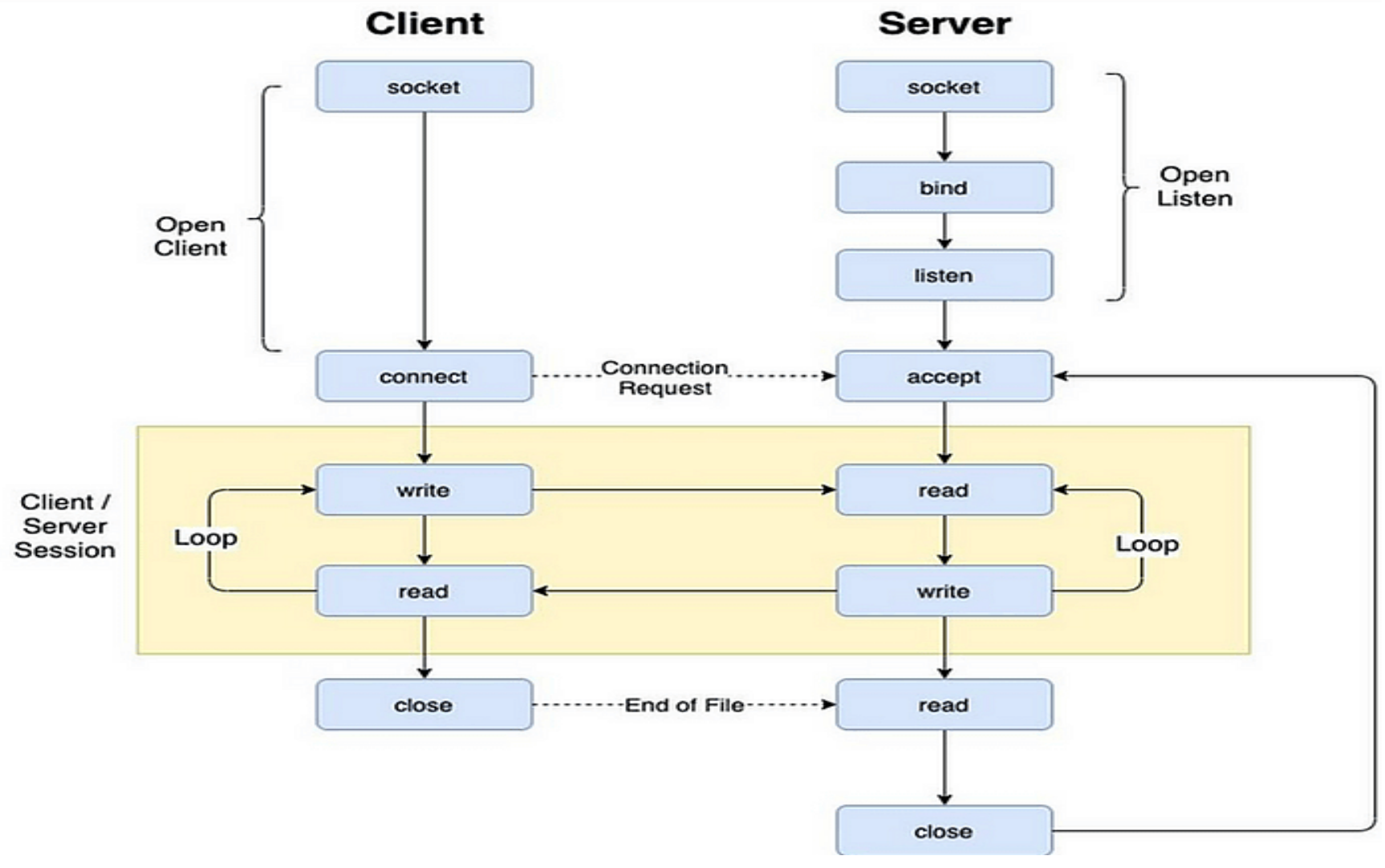
-ال Connection مبين الطرفين وهو بيبدء دول شويه ال packets اللى بيسمح بمرورهم ال Cisco FTD اللى مكون من ال Fire wall وال Snort ودا عشان يعرف نوع ال Connection اذا كان http او Ftp او غيره زي موضحنا ويبنالك ان ال Connection بدء وبعد كدا ممكن ال Fire wall يقفله لو لقى فيه حاجه مش تمام عن طريق مراقبته لل Packets من خلال ال Rule اللى ذكرناها ويبنالك ان ال Connection مفتوح وهو مقفول فالحقيقه .

- تعالى نفهم انهاء ال Connection مبين ال Source وال Destination بيتم ازاي عن طريق ال Flags الخاصه بال TCP .

نفترض ان جهاز ال Source خلاص اتواصل مع ال Destination وبعتله اللى هو عاوزه أو استلم منه اللى عاوز وعاوز ينهي ال Connection هتلاقيه بيبعت ال FIN flag لل Destination يقوله انه عاوز ينهي ال Connection فيقوم ال Destination يرض عليه بال Ack دليل على انه تمام استلم ال FIN الخاص بال Source وفهم انه عاوز ينهي ال Connection اللي مبينهم ... وبيقوم ال Destination هو كمان باعت لل Source ال FIN دليل على انه جاهز هو كمان انه ينهي ال Connection وال Source بعد كدا بيقوم باعت لل Destination ال Ack عشان ينهي الاتصال معاه ودي بتكون أخر خطوه مبينهم .



ـ لحد دلوقتي عرفنا ان ال IDS وال IPS المتمثلين فال Snort بيسمح انه يعدي بعض ال Packets وبعد كدا بيشوفها اذا كانت clean ولا malicious وال بياخد القرار النهاءي انه يمررها ولا لاء هو ال Fire wall ... الفكره هنا عاوزين نعدل طريقه البرمجه الخاصه بال NGFW بحيث نعدي البيانات المهمه بتعتنا فالاول ضمن ال Packets ال بتعدي فالاول قبل ميتكشف ال Connection الكامل ليك ونستفيد من حته ان فيه بعض ال Packets بتمر فالاول او بتهرب من ال Snort ... تعالى نفهم ازاي بيحصل Connection مبين جهازين عن طريق ال Sockets ودي تقنيه بتستخدم للتواصل مبين برنامجين على أجهزة مختلفه أو نفس الجهاز بس لازم يكونوا البرنامجين مختلفين .



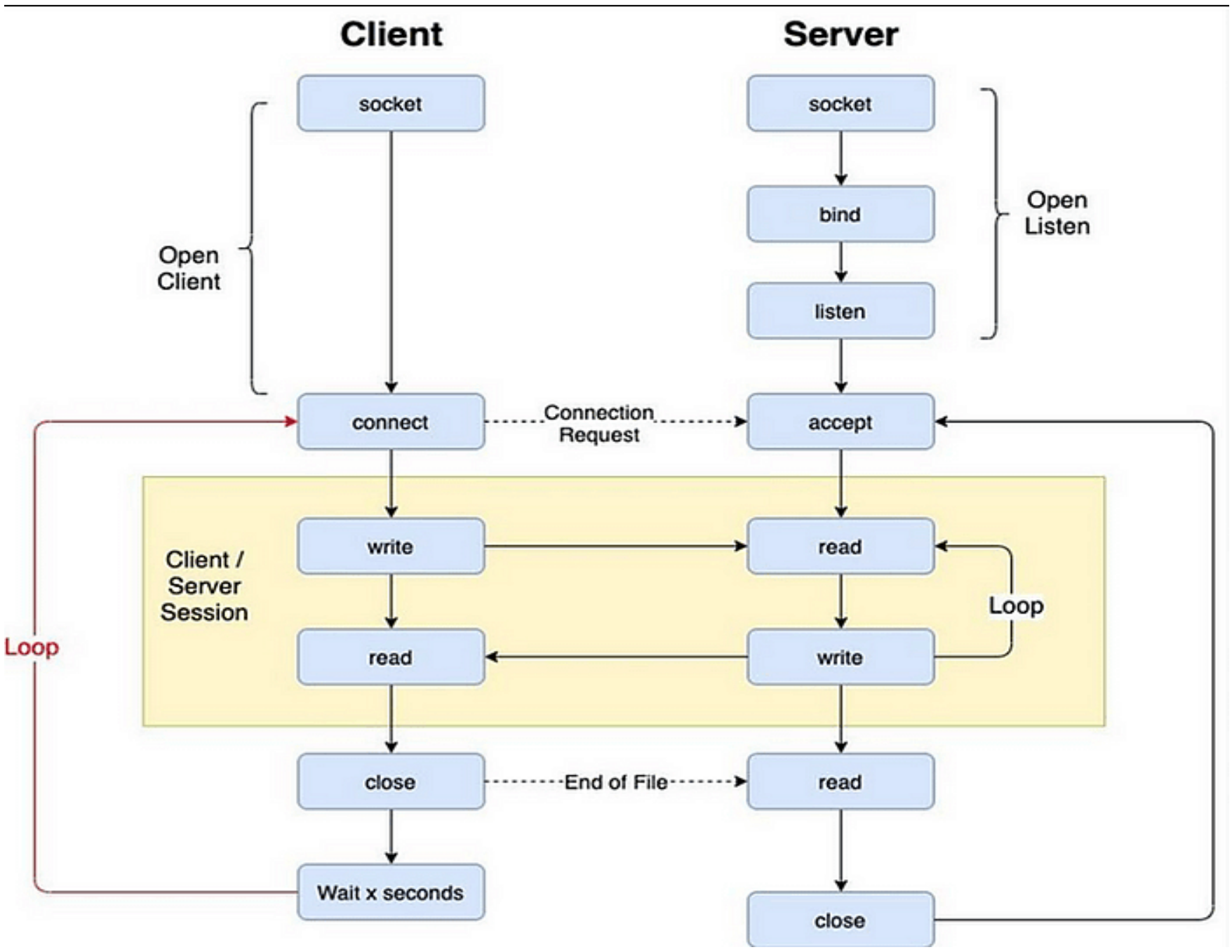
- هتلاقي على الجانب بتاع ال Client عندك ال Socket وال Connect ... وال Socket دا ال Client هو ال بيعمله عشان يجهز نفسه لل Connection ... بعد كدا ال Client بيبعت طلب Connect لل Server ال عاوز يتواصل معاه عن طريق ال Connect .

- هتروح عند ال Server هتلاقي عنده اربع حاجات وهم ال Socket وال Bind وال Listen وال Accept ... بالنسبه لل Socket دا ال Server بيعمله برضه عشان يكون جاهز لاستقبال ال Connection من ال Client .... وال bind دا مسؤول عن تخصيص IP و Port معين لل Socket ال عمله ال Server عشان يستقبل عليه ال Connection ال جايله من ال Client ... بعد كدا ال Server بيدخل فمود ال Listen عشان يسمع اي requests جيالله من ال Clients ... نروح لاخر جزء وهو ال Accept لما بيوصل لل Server ال Request من ال Client بيوافق عليه وبكدا يتم ال Connection مبينهم .

- كدا ال Connection نشأ بين ال Client وال Server واتفتح بينهم Session ... نيجي للجزء الاصفر ال قدامك فالصورة ...

ال Client بيبعت لل Server ال Data عن طريق ال Write وببيدء ال Server يستلم منه ال Data ويقراها عن طريق ال Read ... وال Server يبعت الرد لل Client بال Write ويستلمها منه ال Client بال Read اللى هو يقرأ الرد بتاع ال server عليه ... مره دا يكتب والتاني يستلم منه والعكس صحيح ... العمليه دي بتكون بشكل Loop يعني يقدروا يكرروها كذا مره عشان يتبادلوا ال data براحتهم وفالنهايه لما يحب اي طرف انه ينهي ال Connection بيبعت للطرف التاني ال Close عشان ينهي ال Connection وبكدا يكون ال Connection انتهي بعد اما تبادل ال Data بين الطرفين .

ـ احنا بقا ك **Attackers** هنعمل ايه ... كالاتي فالمثال ال هيتشرح .



ـ هنعمل نفس الخطوات ال اتشرحت فوق عشان يتم ال **Connection** ويحصل تبادل لل **Data** مبين الطرفين ولكن الفكره هنا اننا نعمل ال **Connection** مع ال **Server** ونبعتله ال **Data** ونستلم منه الرد وبعدين نعمل **Close** لل **Connection** وبعد كدا نستنى شويه ونعيد نفس الكلام تاني دا بيعمل زي لخبطه لانظمه ال **IDS** وال **IPS** ومتكشفش ال **Connection** بتاعك بسرعه ودا الغرض من التكرار انك تلغبطه تخليه يركز مع ال **Data** بتعتك وبعدين تبعتله **Data** تانيه وراها علطول عشان فيبقا عامل زي المشتت اللى فقد تركيزه فتعمله زي **error** فالنظام اللى بيمشي عليه ودا اللى بيخلينا نتخطى نظام ال **Detect** السريع الموجود فالاجهزة دي ... فأنت ك **Client** قفلت ال **Connection** مع ال **Server** استنى ثواني وارجع عيده تاني .

ـ بعد اما اتكلمنا عن كل جزء يخص ال Attack وشرحنا تفاصيله تعالى ننفذه ... عندنا Tool قويه لسه نازله 2024 يعني حديثه تقدر تنزلها فال Kali بتنفذلنا ال Attack بتعنا وهي ال frag tunnel عباره عن أداه مصممه بال Python بتوجه ال Connection ف Tunnel من خلال TCP Protocol عشان تعملنا Bypass لل NGFW بالطريقه اللى ذكرناها ... بتعمل Tunnel مبين ال Source وال Destination بيمرر ال Connection ال مبينكم بدون مال NGFW يشك فحاجه فال Connection ويعملك Block .

ـ تعالى نشوف طريقه عمل ال Operating System الخاص بال frag tunnel ونفهم بتتعامل ازاي مع ال Packets ... العمليه دي بتم على اربع خطوات وهم ال Data fragmentation وال Multi session transmission وال Data reassembly وال final Delivery ... أول مرحله معانا ال data fragmentation وهنا ال data ال جايه من ال APP من ال Source وعاوزه تروح لل Destination بتتقطع لاجزاء صغيره أكنك بتفك ال Puzzle كدا تماما ركز عشان هنجمعهم قدام زي ال Puzzle تماما .

ـ بعد كدا عندنا ال Multi – Session transmission ودي بيحصل فيها ان كل جزء من أجزاء ال Data ال اتقسمت بتتبعت منفصله في packet لوحدها ب Session خاصه بيها بدل مكل ال Data تتبعت ف Session واحده ... بعد كدا بنعمل ال Data reassembly اللى هو بنجمع ال Data اللى قسمناها لأجزاء من تاني اللي هو جمعنا أجزاء ال Puzzle اللى فككناها عند ال Destination هناك ... وبعد كدا تيجي المرحله الاخيره وهي ال Final Delivery وهي ان بعد أجزاء ال Data متتجمع من تاني وترتب نفسها بيتم ارسال ال data لل Destination أكنها محصلهاش تجزءه من أساسه .

ـ تعالى ننزل الاداه من GitHub عن طريق ال git clone عندنا فال kali ونشوف ازاي نستخدمها.

```
┌──(abdelnasser㉿abdelnasser)-[~/Desktop/fragtunnel]
└─$ git clone https://github.com/efeali/fragtunnel.git
Cloning into 'fragtunnel' ...
remote: Enumerating objects: 42, done.
remote: Counting objects: 100% (42/42), done.
remote: Compressing objects: 100% (40/40), done.
remote: Total 42 (delta 13), reused 5 (delta 1), pack-reused 0 (from 0)
Receiving objects: 100% (42/42), 2.36 MiB | 2.38 MiB/s, done.
Resolving deltas: 100% (13/13), done.
```

ـ عاوزين نكون ال Tunnel Server ال هنبعت من خلاله ال Data بتعتنا ... ودا عن طريق ال Command دا ...

Python fragtunnel.py -b (interface IP) : (port to listen) -v

ـ ال option ال -b دا اختصارل bind ودا معناه اننا عاوزين نحدد ال IP وال Port اللى الServer بتعنا هيستقبل ال Connection عليه وليكن مثلا ال IP هو 127.0.0.1 وال port هو 8080 الخاص بال Http .... وال option -v دا اختصار ل verbose ودا معناه انه بيشغل الوضع التفصيلي لل Tool عشان يجبلك تفاصيل أكتر .

```
┌──(abdelnasser㉿abdelnasser)-[~/Desktop/fragtunnel]
└─$ sudo python3 fragtunnel.py -b 127.0.0.1:8080 -v
Verbose mode
bind port is 8080
Binding fragmented server on 127.0.0.1:8080
Tunnel server listening on port 8080
```

ـ فالخطوه ال فاتت عملنا ال Server الخاص بال Tunneling ال هيستقبل من ال Client ال Data ... تعالى نعمل ال Setting بتاعت ال Tunnel الخاصه بال Client عشان يستقبل ال Data من ال Server عن طريق ال Tool بتعتنا عن طريق ال Command دا ...

```
Python fragtunnel.py -p ( local port to listen) -t (
target server address : target server port ) -T (
tunnel Server address : tunnel server port )
```

ـ ودا مثال على انشاء ال Tunnel الخاصه بال Client ....

```
Python fragtunnel.py -p 1234 -t Website.com : 80 -T
127.0.0.1 :8080
```

ـ دا معناه اننا حطينا ال Local port على جهازنا اللى ال Tool هتعمل listen عليه عشان تستقبل الConnections ال بتجيلها اللى هو 1234 يعني لو فيه App معين عاوز يستخدم ال Tunnel هيبعت على port 1234 .... بعد كدا بتحط ال IP أو ال Domain الخاصين بال Target اللى عاوز تتواصل معاه اللى هو ال Destination اللى هو ال Server بتاع uber وليكن وبتديله ال Port 80 يعني الاتصال بتاعك يروح على port 80 الخاص بال Http ... بعد كدا بنحط IP وport ال Server اللى عملناه فوق اللى مشغلين عليه ال Tunnel ال هو كان 127.0.0.1 ومعاه خد بالك نفس ال port اللى كان 8080

ـ وبمجرد متشغل ال Client وتتصل بال Server اللى عملناله ك Tunnel هتقدر تتواصل مع ال Target كأنك متصل بيه بشكل مباشر بدون وسيط مبينكوا كأن ال Tunnel بتاع ال Server اللى عملناه مش موجود أصلا بس فالحقيقه كل حاجه بتمر من خلال ال Tunnel الخاصه بال Server .

```
┌──(abdelnasser㉿abdelnasser)-[~/Desktop/fragtunnel]
└─$ sudo python fragtunnel.py -p 1234 -t [redacted]:80 -T 127.0.01:8080 -v
Verbose mode
Local server listening on port 1234
```

- تعالى نأكد على خطواتنا كدا ونشوف هل فعلا نجحنا اننا نعمل Tunnel اللى هنعدي فيه ال Data بتعتنا وكله تمام ولا لاء ...

```
┌──(abdelnasser㉿abdelnasser)-[~]
└─$ curl -I http://localhost:1234
HTTP/1.1 200 OK
Date: Fri, 15 Nov 2024 05:29:20 GMT
Server: Apache
Content-Type: text/html;charset=UTF-8
```

- هتلاقي الرد اللى جالك هو 200 ودا معناه ان ال Frag tunnel شغاله بشكل صحيح وقدرنا نعمل Connection بال Target بتعنا من خلال ال Client على ال Local port 1234 .

- كدا عملنا ال Tunnel بين جهاز ال Client وليكن ال Kali Linux وبين ال Server ال هو خاص بال Destination ... بعد كدا ال Client بيستخدم ال Frag tunnel عشان عشان يبدء ال Connection مع ال Destination من خلال ال tunnel وبيتم ارسال ال Data فال Tunnel على port 80 زي موضحنا قبل كدا ... ودا بيسمح لل Client انه يتصل بال Destination اللى هو ال Target كأنه متصل مع ال Local Server ....

ـ لو شغلت اداه زي ال TCP Dump وانت مشغل ال frag tunnel هتلاقي ان كل ال data بيتم تمريرها من خلال ال Server اللى عملناه اللى كان ال IP الخاص بيه 127.0.0.1 ودا معناه ان تم توجيه ال Traffic من خلال ال Tunnel اللى بين ال Client وجهاز ال Target اللى هو ال Destination .... ناخد مثال لو فتحنا connection مع amazon وليكن هو ال Target ال عاوز تتواصل معاه وتعمل عليه Scanning واللى هتحط ال IP الخاص بيه فال Setting فوق على حسب ال Target اللى عاوز تتواصل معاه بتغير ال IP بتاع ال Destination وعاوزين نشوف ال packets ال طالعنا من عندنا رايحه لل Destination من خلال ال TCP Dump

```
02:01:13.974032 IP [redacted].41462 > s3-console-us-standard.console.aws.amazon.com.1234: Flags [S], seq 2
314043594, win 64240, options [mss 1460,sackOK,TS val 3912567055 ecr 0,nop,wscale 7], length 0
02:01:14.020204 IP [redacted].42716 > 192.168.226.2.domain: 55608+ PTR? 103.242.251.205.in-addr.arpa. (46)
02:01:14.132728 IP [redacted].domain > 192.168.226.141.42716: 55608 1/0/0 PTR s3-console-us-standard.console
.aws.amazon.com. (105)
02:01:14.982847 IP [redacted].41462 > s3-console-us-standard.console.aws.amazon.com.1234: Flags [S], seq 2
314043594, win 64240, options [mss 1460,sackOK,TS val 3912568065 ecr 0,nop,wscale 7], length 0
02:01:16.006931 IP [redacted].41462 > s3-console-us-standard.console.aws.amazon.com.1234: Flags [S], seq 2
314043594, win 64240, options [mss 1460,sackOK,TS val 3912569089 ecr 0,nop,wscale 7], length 0
02:01:16.712961 IP s3-console-us-standard.console.aws.amazon.com.1234 > 192.168.226.141.41462: Flags [R.], seq
185018546, ack 2314043595, win 64240, length 0
```

ـ هتلاحظ ان كل ال Connection ال طالعه من ال Client بتروح لل Server بشكل مباشر ومنه ل Amazon وفالطريق بتم عمليه تجزءه ال packets وتجميعها زي مشرحنا فوق وبكدا مفيش Connection مباشر بين ال Client وال Target لأن كل ال Traffic بيتم توجيهه من خلال ال Server Tunnel ال عملناه ال شغال فيه ال frag tunnel اللى بيجزء ال packets ويجمعها عشان نتخطي عمليه ال Deep investigation الخاصه بال NGFW وهو بيتعامل مع ال Target ولكن ال Client ملهوش صله مباشره بال Target ... وبس كدا وبكدا نكون عملنا ال Attack بتعنا من خلال ال frag tunnel tool وعملنا Bypass لل NGFW .

- الخلاصه ... اننا فى مرحله زي ال reconnaissance أو ال Scanning على Server ل target ما فنبقا عاوزين نعرف ال ports المفتوحه عند ال target دا وال Services اللى شغاله عليها لكن بتواجهنا مشكله وهي ال Fire walls لما تيجي تعمل connect بال Server بتلاقيه مانعك والسبب انه NGFW بيعمل deep investigation فحص بشكل عميق لل packets بسبب ال IDS وال IPS المدمجين فيه ... انظمه ال IDS وال IPS بتسمح بمرور بعض ال packets ووصولها لل Server ... فأحنا بنستغل ثغره فال NGFW وهي انه بيسمح بمرور بعض ال packets لوقت قليل قبل مياخد قرار هيعدي ال Packets ولا يعملها Block ودا عيب فال system ذات نفسه .... كل دا بنقدر ننفذه عن طريق Tool ال frag tunnel اللى بتعمل fragment لل packets عشان تخدع ال NGFW وتخليه يعدي بعض ال packets اللى بدورها بتوصل لل destination اللى هو هنا ال server target وتفتحلنا Connection معاه ... وبس كدا يارب أكون فدتك بشيء .

- ومتنساش كالعاده ذكر الله والصلاه عالنبي محمد صلي الله عليه وسلم والدعاء الصادق لأخواتنا المستضعفين في غزه ولبنان والسودان واليمن وسوريا بأن ينصرهم الله ويثبت أقدامهم ... ومتنساش المقاطعه ودعم أخواتك بكل ما تستطيع .