Proxies

Շատ մարդիկ տարբեր կարծիքներ ունեն այն մասին, թե ինչ է պրոքսին.

Անվտանգության մասնագետները անցնում են HTTP Proxies (BurpSuite) կամ SOCKS/SSH Proxy (Chisel , ptunnel , sshuttle) միջոցով:

Վեբ մշակողները օգտագործում են Cloudflare-ի կամ ModSecurity-ի նման պրոքսի սերվերներ՝ վնասակար երթևեկությունը արգելափակելու համար:

Միջին մարդիկ կարող են մտածել, որ պրոքսին օգտագործվում է ձեր գտնվելու վայրը թաքցնելու և մեկ այլ երկրի Netflix կատալոգ մուտք գործելու համար:

Իրավապահ մարմինները հաճախ լիազորված անձանց են վերագրում անօրինական գործունեությունը:

Վերոնշյալ բոլոր օրինակները ճիշտ չեն: Proxy սերվերը կապակցման կենտրոնում գտնվող սարք կամ ծառայություն է, որը գործում է որպես միջնորդ: mediator կարևորագույն տեղեկատվություն է, քանի որ դա նշանակում է, որ կենտրոնում գտնվող սարքը պետք է կարողանա ստուգել երթևեկության բովանդակությունը: mediator լինելու հնարավորության բացակայության դեպքում սարքը տեխնիկապես gateway է, այլ ոչ թե պրոքսի:

Վերադառնալով վերոնշյալ հարցին՝ միջին մարդը սխալ պատկերացում ունի այն մասին, թե ինչ է պրոքսին, քանի որ, ամենայն հավանականությամբ, օգտագործում է VPN՝ իր գտնվելու վայրը թաքցնելու համար, ինչը տեխնիկապես պրոքսի չէ: Մարդկանց մեծ մասը կարծում է, որ երբ IP հասցեն փոխվում է, դա պրոքսի է, և շատ դեպքերում, հավանաբար, ավելի լավ է չուղղել դրանք, քանի որ դա տարածված և անվնաս սխալ պատկերացում է: Դրանք ուղղելը կարող է հանգեցնել ավելի երկարատև զրույցի, որը կհանգեցնի tab-երի և space-երի, emacs և vim միջև կամ կբացահայտի, որ ինքը nano օգտատեր է:

Եթե դժվարանում եք հիշել սա, պրոքսիները գրեթե միշտ կաշխատեն OSI մոդելի 7-րդ մակարդակում: Կան պրոքսի ծառայությունների բազմաթիվ տեսակներ, բայց հիմնականներն են՝

- Dedicated Proxy / Forward Proxy
- Reverse Proxy
- Transparent Proxy

Dedicated Proxy / Forward Proxy

Նվիրված պրոքսի / փոխանցող պրոքսի

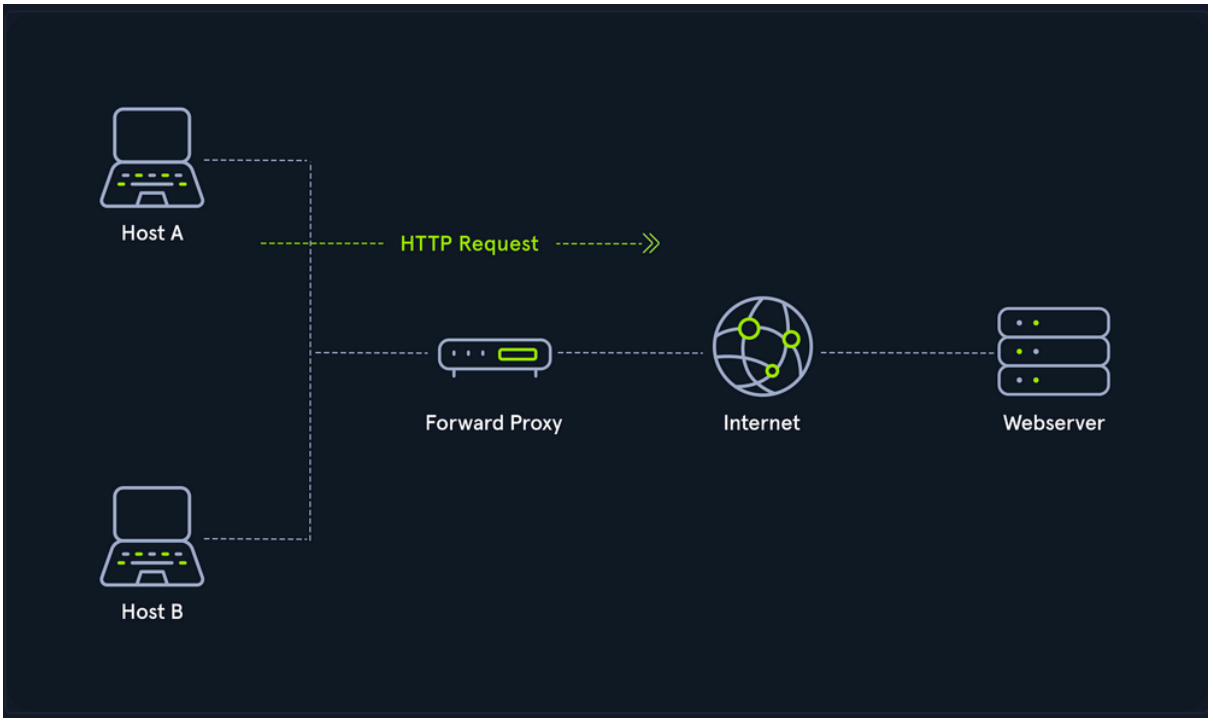
Forward Proxy այն է, ինչ մարդկանց մեծ մասը պատկերացնում է որպես պրոքսի: Փոխանցող պրոքսին այն է, երբ հաճախորդը հարցում է ուղարկում համակարգչին, և այդ համակարգիչը կատարում է հարցումը:

Օրինակ, կորպորատիվ ցանցում զգայուն համակարգիչները կարող են չունենալ ուղիղ մուտք դեպի ինտերնետ: Կայք մուտք գործելու համար նրանք պետք է անցնեն պրոքսիի (կամ վեբ ֆիլտրի) միջով: Սա կարող է լինել աներևակայելիորեն հզոր պաշտպանության գիծ վնասակար ծրագրերի դեմ, քանի որ այն ոչ միայն պետք է շրջանցի վեբ ֆիլտրը (հեշտությամբ), այլև պետք է proxy aware կամ օգտագործի ոչ ավանդական C2 (վնասակար ծրագրի միջոցով առաջադրանքների վերաբերյալ տեղեկատվություն ստանալու միջոց): Եթե կազմակերպությունն օգտագործում է միայն FireFox , ապա պրոքսիի մասին տեղյակ վնասակար ծրագրեր ստանալու հավանականությունը քիչ հավանական է:

Ինտերնետային զննարկիչները, ինչպիսիք են Internet Explorer-ը, Edge-ը կամ Chrome-ը, բոլորը լռելյայնորեն ենթարկվում են "System Proxy" կարգավորումներին: Եթե վնասակար ծրագիրը օգտագործում է WinSock (բնիկ Windows API), այն, հավանաբար, պրոքսիի մասին կիմանա առանց որևէ լրացուցիչ կոդի: Firefox-ը չի օգտագործում WinSock և փոխարենը օգտագործում է libcurl , որը թույլ է տալիս օգտագործել նույն կոդը ցանկացած օպերացիոն համակարգի վրա: Սա նշանակում է, որ վնասակար ծրագիրը պետք է փնտրի Firefox-ը և գործարկի պրոքսիի կարգավորումները, ինչը վնասակար ծրագիրը շատ քիչ հավանական է, որ անի:

Այլընտրանքորեն, վնասակար ծրագիրը կարող է օգտագործել DNS-ը որպես c2 մեխանիզմ, բայց եթե կազմակերպությունը վերահսկում է DNS-ը (ինչը հեշտությամբ կարելի է անել Sysmon-ի միջոցով), այս տեսակի տրաֆիկը պետք է արագ բռնագրավվի:

Forward Proxy-ի մեկ այլ օրինակ է Burp Suite-ը, քանի որ մարդկանց մեծ մասն այն օգտագործում է HTTP հարցումները փոխանցելու համար: Այնուամենայնիվ, այս ծրագիրը HTTP Proxies-ների շվեյցարական բանակային դանակն է և կարող է կարգավորվել որպես հակադարձ պրոքսի կամ թափանցիկ:



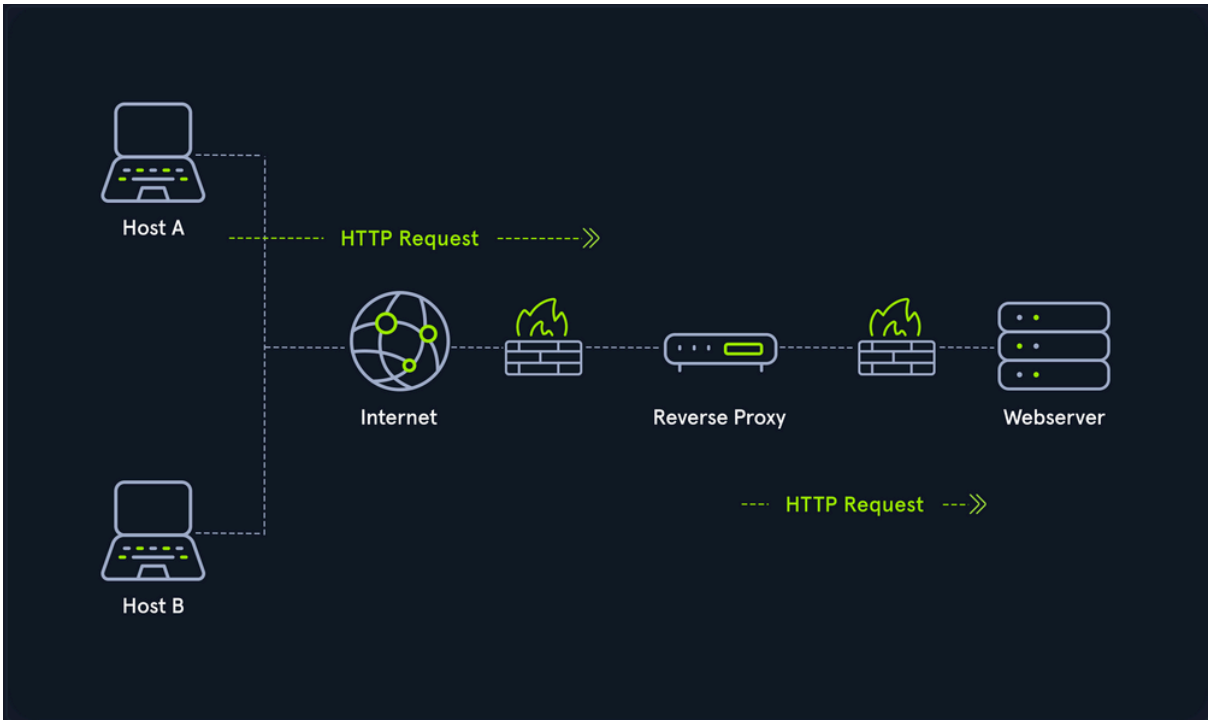
Reverse Proxy Հակադարձ պրոքսի

Ինչպես գուցե կռահել եք, reverse proxy Forward Proxy ի հակառակն է: Այն նախատեսված չէ ելքային հարցումները զտելու համար, այլ զտում է մուտքայինները: Reverse Proxy ամենատարածված նպատակը հասցեն լսելն ու այն փակ ցանցին վերահասցեավորելն է:

Շատ կազմակերպություններ օգտագործում են CloudFlare-ը, քանի որ ունեն հզոր ցանց, որը կարող է դիմակայել DDOS հարձակումների մեծ մասին: Cloudflare-ն օգտագործելով՝ կազմակերպությունները հնարավորություն ունեն զտելու իրենց վեբ սերվերներին ուղարկվող տրաֆիկի քանակը (և տեսակը):

Ներթափանցման փորձարկողները կկարգավորեն հակադարձ պրոքսիները վարակված վերջնակետերի վրա: Վարակված վերջնակետը կլսի մի պորտի վրա և կուղարկի ցանկացած հաճախորդ, որը միանում է պորտին վարակված վերջնակետի միջոցով հարձակվողին: Սա օգտակար է firewall-ները շրջանցելու կամ գրանցումից խուսափելու համար: Կազմակերպությունները կարող են ունենալ IDS (Intrusion Detection Systems), որոնք դիտում են արտաքին վեբ հարցումները: Եթե հարձակվողը մուտք է գործում կազմակերպություն SSH-ի

միջոցով, հակադարձ պրոքսին կարող է վեբ հարցումներ ուղարկել SSH թունելի միջոցով և խուսափել IDS-ից:
Մեկ այլ տարածված հակադարձ պրոքսի է ModSecurity ն՝ Web Application Firewall (WAF): Վեբ հավելվածների firewall-ները ստուգում են վեբ հարցումները չարամիտ բովանդակության առկայության համար և արգելափակում են հարցումը, եթե այն չարամիտ է: Եթե ցանկանում եք ավելին իմանալ այս մասին, խորհուրդ ենք տալիս կարդալ ModSecurity Core Rule Set-ը , քանի որ դա հիանալի մեկնարկային կետ է: Cloudflare-ը նույնպես կարող է գործել որպես WAF, բայց դա անելու համար անհրաժեշտ է թույլ տալ նրանց վերծանել HTTPS երթևեկությունը, ինչը որոշ կազմակերպություններ կարող են չցանկանալ:



(Non-) Transparent Proxy

(Ոչ) թափանցիկ պրոքսի

Այս բոլոր պրոքսի ծառայությունները գործում են կա՛մ transparently , կա՛մ non-transparently :

transparent proxy դեպքում հաճախորդը չգիտի դրա գոյության մասին: Թափանցիկ պրոքսին խլում է հաճախորդի ինտերնետին ուղարկվող հաղորդակցման հարցումները և հանդես է գալիս որպես փոխարինող

ինստանս: Արտաքինից, թափանցիկ պրոքսին, ինչպես ոչ թափանցիկ պրոքսին, հանդես է գալիս որպես հաղորդակցման գործընկեր:

Եթե դա non-transparent proxy է, մեզ պետք է տեղեկացնել դրա գոյության մասին: Այդ նպատակով մեզ և մեր կողմից օգտագործվող ծրագրաշարին տրվում է պրոքսիի հատուկ կարգավորում, որը ապահովում է, որ ինտերնետ երթևեկությունը նախ ուղղված լինի պրոքսիին: Եթե այս կարգավորումը գոյություն չունի, մենք չենք կարող կապ հաստատել պրոքսիի միջոցով: Սակայն, քանի որ պրոքսին սովորաբար ապահովում է այլ ցանցերի հետ միակ կապի ուղին, ինտերնետի հետ կապը սովորաբար անջատվում է առանց համապատասխան պրոքսի կարգավորման: