

# Forum:[Hack Forums](#)

Thread: [Firewall bypass](#)

**SameFish95** - September 21, 2016, 6:53 am

What common strategies are used when trying to infect a firewall protected windows system with a rat?

Is there any port with better chances than others? Some injection methods?

Thank you.

**Slavoj Žižek** - September 21, 2016, 8:15 am

a common way of bypassing the firewall is injecting into something that uses loads of internet (eg. a webbrowser) or a trusted executable

**QU?CKSILVER** - September 21, 2016, 8:53 am

Yes, injecting into an already whitelisted process is the solution, but the problem about injecting into other processes is that it could trigger the antivirus to detect because of suspicious behavior. Unfortunately, most injection techniques are already known by antiviruses.

As for the Windows Firewall, you don't need that shit. It is so easy to bypass.

**SameFish95** - September 22, 2016, 10:17 am

Thanks to both of you for the reply. I'm looking to try to bypass an eventual hardware firewall. I think I will try the injection in browser method since I don't know the target ip and so I can't do a port scan.

**QU?CKSILVER** - September 22, 2016, 10:51 am

(Sep 22, 2016 10:17 AM)kokyx92 Wrote: [\[CITE\]](#) Thanks to both of you for the reply. I'm looking to try to bypass an eventual hardware firewall. I think I will try the injection in browser method since I don't know the target ip and so I can't do a port scan.

If it's a physical firewall then you're going to have to investigate why the firewall is filtering specific outbound traffic.

Many modern firewalls will block connections to botnets/RATs and many other Command and Control stations, so there is a chance that firewall knows the way these software communicate (their traffic, their signatures and such), so that when it sees sketchy traffic going through, it will not let it establish communication or even negotiate with the server.

A way you can evade a firewall's Stateful Packet Inspection, is by encrypting the traffic (Many RATs already do this), but the Firewall will still learn from that traffic and filter it in the future.

**SameFish95** - September 22, 2016, 11:21 am

Wish I could +rep you. Thank you so much!