

Re: what should I do when....

## Re: what should I do when....

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-07/msg00185.html>

---

- *From:* Adriel Desautels <[adriel@xxxxxxxxxxxxx](mailto:adriel@xxxxxxxxxxxxx)>
  - *Date:* Tue, 15 Jul 2008 14:03:27 -0400
- 

Ansgar,

I almost feel like you are trying to create an argument just for the sake of creating an argument. You didn't answer my initial question which was, can you show me a firewall that does *\*secure\** a network? If you know what you're talking about then the answer should be "no".

Secondly, I never asked for any method to prevent the attack scenario that I described, it was a real world example. Your method for preventing the attack would be great in an ideal world, but *\*this\** is not an ideal world. The fact of the matter is that *\*most\** businesses do not restrict outbound SSL traffic and even less of them decrypt and re-encrypt traffic for the sake of outbound monitoring. Not to mention not all of our outbound connections are established over port 443, we can use any port, hell we can even use ICMP or UDP. There are *\*much\** better solutions to the problem of reverse connections anyway.

<http://www.cs.uit.no/~daniels/PingTunnel/> <--- cool stuff.

With respect to your solution, I don't like it. You are creating latency by decrypting, inspecting, and re-encrypting outbound traffic (and do you really think that your *\*monitoring appliance\** will detect our reverse tunnel??). You are creating more work for your employees by setting up white-lists for outbound browsing instead of doing the inverse. Lastly, you are creating what some may consider a vulnerability by decrypting and re-encrypting traffic. What if someone hacks the proxy? Then all of that *\*secure\** ssl content is clear text and theirs for the taking.

The *\*better\** way to prevent people from being compromised is to use something like OSSEC or Cisco's CSA to control the targeted system and limit the possibility of/ease of exploitation. The second thing that should be done is to implement proper security policies and personnel training. You can monitor outbound traffic, but your IDS/IPS devices can only detect what they know to look for, and I know that our attacks and payloads are generally very evasive (IDS is flawed technology and frankly doesn't work as advertised). If you prevent the exploit from working in the first place with OSSEC or CSA then you've defeated most, but not all of the issue.

Firewalls do not secure networks! People who tell people that they do are doing an injustice (its almost a lie). I break into networks for a living, I bypass your security technologies, I circumvent your policies, and I social engineer your people, firewalls aren't a challenge. Thank god I'm one of the good guys right? ;]

Regards,  
Adriel T. Desautels  
Chief Technology Officer  
Netragard, LLC.  
Office : 617-934-0269

Re: what should I do when....

Re: what should I do when....

Mobile : 617-633-3821

<http://www.linkedin.com/pub/1/118/a45>

Join the Netragard, LLC. Linked In Group:

<http://www.linkedin.com/e/gis/48683/0B98E1705142>

---

Netragard, LLC – <http://www.netragard.com> – "We make IT Safe"  
Penetration Testing, Vulnerability Assessments, Website Security

Netragard Whitepaper Downloads:

---

Choosing the right provider : <http://tinyurl.com/2ahk3j>

Three Things you must know : <http://tinyurl.com/26pjsn>

Ansgar -59cobalt- Wiechers wrote:

On 2008-07-11 Adriel Desautels wrote:

A firewall is software running on hardware that is designed to enforce security policies that have little effect on how a hacker breaks into your network. So long as the hacker works within those policies his or her traffic will be passed, and they'll get in.

A firewall is not a system that \*secures\* a network, shielding it from access by unauthorized users, but it might want to be and some people might like to think that it does that effectively. Can you show me one that does \*secure\* a network?

For every security concept you identify threats, break them down into distinct attack scenarios and identify countermeasures for each attack scenario (or decide that you'll live with the risk that the given scenario poses).

During one of our penetration tests I convinced a user to browse to a page hosted on our company website. When they did, their browser was exploited and their computer connected back to me over https. Why did I choose https? I chose https because I knew that the firewall allowed outbound https connections for users. I then used that access to perform distributed metastasis and penetrate other systems. The firewall did not "Secure" the network and "prevent" unauthorized access, we still got in.

There are obviously several ways to deal with this scenario on a firewall-level:

a) Disallow https altogether.

Re: what should I do when....

Re: what should I do when....

- b) Whitelist sites that are allowed to be accessed via https.
- c) Man in the middle: Break the https connection into two connections, one from the client to your proxy, the other from your proxy to the server. Then your proxy can inspect/filter the traffic.

Regards  
Ansgar Wiechers