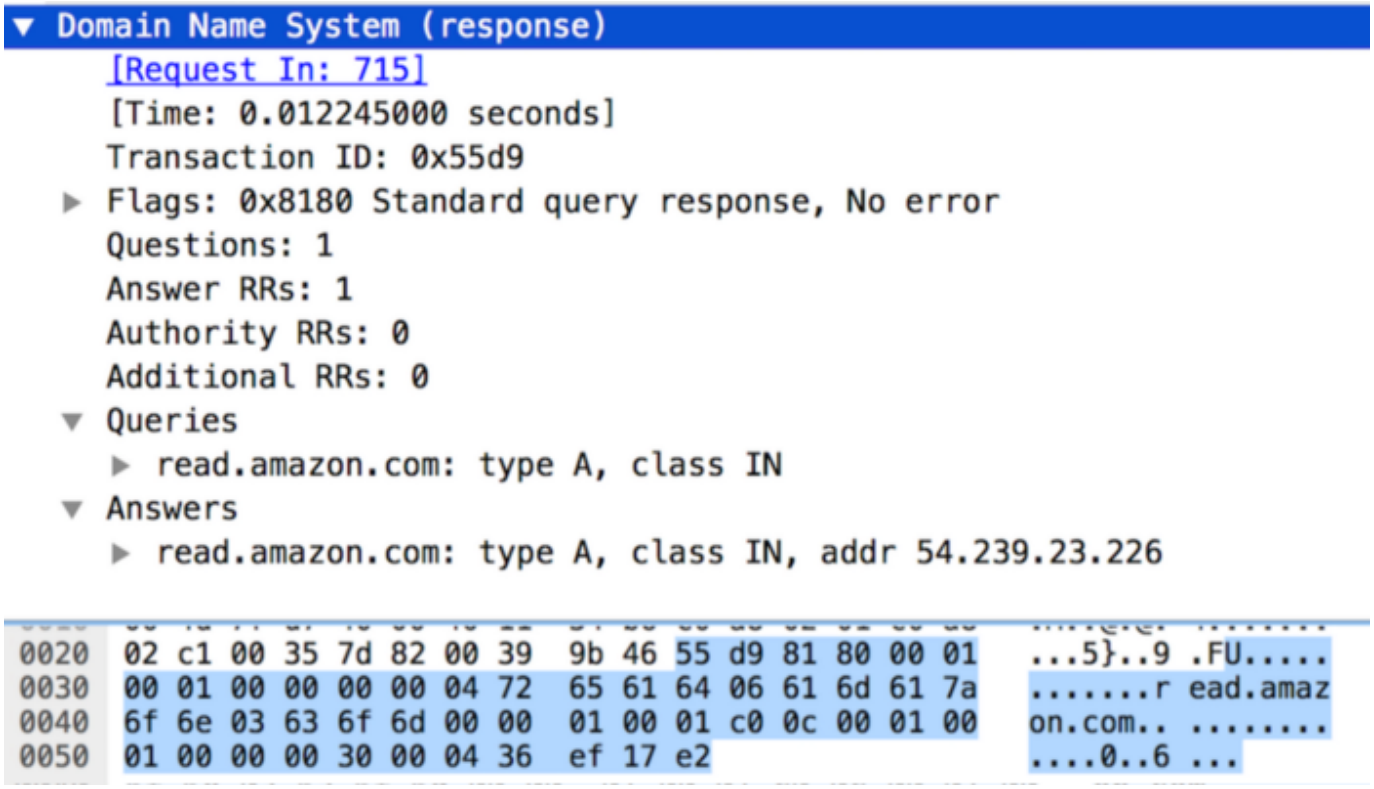
Cloud Security ~ Why Use a VPN for Remote Administration?

Teri Radichel Follow
Dec 18, 2018 · 4 min read ★

Any time you are using public wifi, or in other words a network you don't own and secure yourself that allows anyone to connect, it's a good idea to use a VPN (virtual private network). A VPN provides an authenticated, encrypted connection that hides information in about the sites you are visiting from attackers. This protected connection makes it harder to intercept your connections, steal or read your data, or insert attacks into the traffic as it flows from your system to other sites.

To give you an idea what I'm talking about, let me first show some information retrieved by a sniffer when I navigate to Amazon.com in a web browser. When visiting this site, many different URLs are used to pull

together the content you see when you visit the home page. One of the domain names is read.amazon.com. If I run a sniffer while visiting that web page, without a VPN, I can see the request to this domain name in plain text.



As an attacker there are many ways I can use this information, not to mention any other information sent clear text in payloads of other packets. On an insecure wireless network, anyone with a sniffer could see this traffic.

Even on some of the newer, more secure networks, there may be ways for an attacker to intercept and view this data.

Now let's look at what I see when connected to an IPSEC VPN. All the packets pretty much look like this — because the data is flowing through an encrypted tunnel:

```
0020  02 c1 11 94 11 94 00 6c  00 00 09 ae 99 c5 00 00   .......l ........
0030  08 2f 6c 59 c2 90 f0 ac  9a e7 a7 bf d8 55 ad be   ./lY.... .....U..
0040  fe ee 35 a9 01 a3 63 c6  02 b9 ed 79 69 4c 3b ac   ..5...c. ...yiL;.
0050  48 ac c7 91 ec bb 11 1b  33 c6 5f 2b 83 be d2 55   H....... 3._+...U
0060  34 a0 40 5c ae 0e 4d ab  de 99 9c 55 ef 0c b8 bd   4.@\..M. ...U....
0070  d8 2a 3f 93 4b 09 f0 36  9a ab 90 8c 8c 36 0d e8   .*?.K..6 .....6..
0080  46 eb 3a 1a fc 9a fc c5  67 3f 7f b1 ae 5c         F.:..... g?...\
```

In addition to limiting exposed data while using an insecure network, A VPN also allows network administrators to create firewall rules for your company systems, to allow traffic only from the VPN connections rather than the whole Internet. Why does this matter? Any time the network rules expose a host to the Internet, any open ports will be scanned and attacked. You can reduce the "attack surface" (what an attacker can attack) by limiting what you expose to the Internet to only what is required. I talked

about this in a presentation on AWS network security at our AWS meetup in Seattle. Here's the most critical slide:

If you don't believe your systems are subject to attacks when exposed to the Internet, go into your AWS account right now. Start up an EC2 instance. Turn on VPC Flow Logs and wait about 5 minutes. Then look at all the traffic that is trying to hit the system you just turned on in the VPC Flow Logs.

Next, turn on SSH or RDP and open up the network to provide access to those services from the Internet. Turn on Amazon GuardDuty. Then wait to see how long it takes GuardDuty to report RDP or SSH brute force attacks. In most cases, it will be less than one day, if not less than one hour.

What if we need to allow someone to administer a system running on AWS, Azure, or Google Cloud from varying remote locations but don't want to expose SSH and RDP to the entire Internet? One option would be to provide VPN access, which allows the person to connect from anywhere on the Internet to the corporate network. Then only allow access to the Bastion host via RDP or SSH from the corporate network. The VPN will be another layer the attackers have to get through before they can get to RDP or SSH.

One concern with a VPN is the fact that traffic has to be back-hauled back to the corporate network however some creative cloud architecture solutions could get around this problem. Another issue is that you'll still need to protect your VPN endpoint from attacks similar to those used while cloud penetration testing to simulate real-world attacks. You should implement two-factor authentication with your VPN solution and ensure you are using a secure VPN configuration.

Teri Radichel — Follow me on Medium and Twitter @teriradichel

___

Check out the book I'm writing: Cybersecurity for Executives

___

*Follow me for future blog posts on cloud security, or sign up for **cloud security training** to learn more. © 2nd Sight Lab 2019*

Upcoming events where you can hear Teri Radichel speak about cloud security:

AWS RE:INFORCE ~ Are you ready for a cloud pentest?

IANS Seattle Information Security Forum (Cryptojacking, Cloud Migration, Google Cloud) (June 12–13)

IANS Charlotte Information Security Forum (September 25–26)

IANS Houston Information Security Forum (September 11)

Bienvenue au congrès ISACA Québec 2019

…and of course she's usually at the Seattle AWS Architects and Engineers Meetup sponsored by 2nd Sight Lab!

Past Cloud Security Presentations (Videos)

RSA ~ Red Team vs. Blue Team on AWS with Kolby Allen

AWS re:Invent ~ RedTeam vs. Blue Team on AWS with Kolby Allen

Microsoft Build ~ DIY Security Assessment with SheHacksPurple

VPN | Cloud Security | Cloud Security Training | Aws Security | Azure Security

50 claps

WRITTEN BY

Teri Radichel

Follow

Cloud Security Training and Consulting | GSE 240, GSEC, GCIH, GCIA, GCPM, GCCC, GREM, GPEN, GXPN | AWS Hero | Infragard | IANS Faculty | 2ndSightLab.com

Cloud Security

Follow

Cloud security blog by 2nd Sight Lab ~ Cloud Security Training, Pen Testing and Consulting

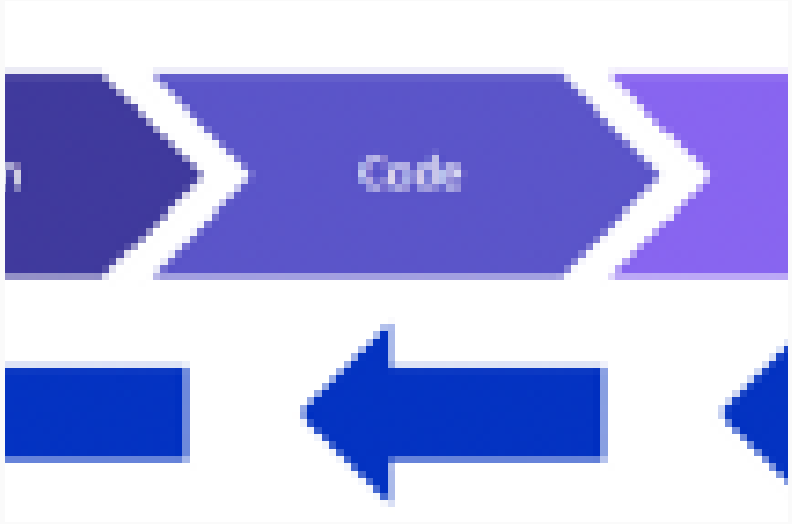
More From Medium

Related reads

Pushing Left, Like a Boss: Part 1

SheHacksPurple in Code Like A Girl
Jul 8, 2018 · 5 min read

432



Related reads

PoweredLocal's DNS based Firewall

Michael Jankie in WHAT THE FI. BY...
Feb 18 · 6 min read

13

Related reads

Putting Sysmon v9.0 AND/OR Grouping Logic to the Test

Roberto Rodriguez in Posts By...

Feb 20 · 12 min read

47