Proactive Network Security

Moving to Network Zero Trust Architecture With SmokeNet™

Introduction

It seems like we read about cybersecurity issues every week. Ransomware is a problem that can wipe a company out. Introspective Networks has developed a technology called SmokeNet that significantly reduces Cybersecurity risk.

The biggest cybersecurity risks currently are networks where remote hacking is happening. SmokeNet comprehensively removes this risk by not trusting the network. SmokeNet creates an impervious tunnel to protect your data from all network threats. SmokeNet is more than just encryption.

Built as a reaction to the 2013 “Snowden” NSA leaks, SmokeNet has nearly a decade of development with over five years of commercial usage and multiple granted patents. In all cases, it removes issues that lead to cybersecurity problems. It is a rethinking of the cybersecurity problem from the son of a Bell Labs fellow who has been contemplating these problems for over four decades as an active thought leader.

For networking, tunnels for your private network become an impenetrable shield around your data. SmokeNet has been independently verified to have zero network vulnerabilities. This is accomplished by making data invisible to attackers. It is the only product with this level of security. This does the same thing for your network edge. No one will know your computer is even connected to the internet.

From personal security to enterprise business, SmokeNet is the first comprehensive, proactive cybersecurity platform available to the general public with Department of Commerce approval including a positive NSA review.

Current State Of Cybersecurity - Cyber Offense

In today’s cybersecurity world, it should be clear things don’t work well. This is because the firewall and VPN solutions are antiquated at over 25 years old. Very little has been done to update this situation. The state of affairs in the 1990’s revolved around Cyber Offense - the ability to collect and surveil large amounts of data. This was the approach the US Justice Department put in place with their Carnivore system and program. The fear was criminals would be able to hide their information exchanges through the Internet. To counter this, the NSA and NIST created encryption standards as well as methods to record data en masse. Congress obliged with the CALEA law mandating interception and data recording capabilities be added to the equipment that runs the Internet. Those capabilities are ineffective if the encryption can not

be cracked by law enforcement. So, the fact that our 25 year old encryption was designed to be cracked is self-evident.

By requiring commercial standardization of encryption, law enforcement's ability to intercept and decrypt data was ensured. The encryption was sold as “theoretically insecure” with a litany of half truths about why it could not be cracked. Since these encryption standards are derived from math with a, relatively speaking, short key, they are provably at risk from three attacks - mathematical proof, brute force, and key theft. No one argues these are not real issues. The rules of cybersecurity need to be very strict - if something is theoretically insecure, it is insecure. Simply put, current encryption standards are designed to be cracked. Of course, after 25 years, others have figured out how to defeat these encryption methods. With Cloud Computing, where the cloud provider holds a copy of the keys and support staff can be manipulated into giving up the keys (through social engineering or other means), key theft has become one of the most common methods for conducting Ransom attacks. The larger the company, the more employees, the more likely an attack will work.

All of this culminates into a hostile Internet left open by Offensive Cybersecurity practices. The 2013 “Snowden” NSA leaks exposed the real extent of what has been done to enhance offensive cybersecurity capabilities. There were backdoors created in systems by large corporations at the request of the NSA, social engineering methods to collect VPN keys, and other techniques to take advantage of existing system vulnerabilities. There is a clear line between these leaks and the rise of Ransomware attacks.

The leaks were a call to action for Introspective Networks founder Anthony Scott Thompson. Anthony, who has developed expertise in Internet protocols and cybersecurity over nearly four decades, intimately understands how the original Internet protocols, and US legislation, have evolved with inherent vulnerabilities that hackers take advantage of. His father, Dr. Larry F. Thompson, a Bell Labs Fellow, who also served on the DoD Science Advisory Board in the late 70’s and 80’s, taught that even highly sophisticated algorithms can not be used for encryption because a proof, however complex, would reveal the encryption key. You also need the proof to validate the algorithm so whoever created the encryption algorithm would immediately have the means to defeat it. With that knowledge, Anthony developed SmokeNet. This was done with a counter approach - Cyber Defense. As of May 12th, 2021, the US is moving to Cyber Defense by the "Improving the Nation's Cybersecurity" executive order. That title is exactly what SmokeNet does through impervious networking tunnels with stealth networking technology.

After the "Improving the Nation's Cybersecurity" executive order which moves the US to Cyber Defense, a government plan first contemplated in the early 2000’s - Zero Trust cybersecurity - was put into action. Zero Trust, as a concept, is very simple - you don’t trust anything or anyone, and you assume an attacker is already present within the network. SmokeNet fits this model perfectly and, coincidentally, hits on many of the recommendations made 20 years ago.

To begin, for networking, the first thing is to not use the Internet as directly prescribed. The protocols were designed for diagnostics and not for security. The original ARPANET architects

never contemplated that the network would be used for ecommerce, cloud computing, video/voice communications or streaming artistic content. The secure networks of tomorrow must leverage existing infrastructure but without exposing the streams of data to interception, recording and decryption - the exact things the Justice Department in the 90's enabled for law enforcement are now being used by criminals.

Proven Uncrackable Encryption

Shortly after hanging the first wires off telegraph poles, we started "wiring" money. Soon after, people climbed those poles to start intercepting and stealing the money transfers. To counter this problem, a Wells Fargo employee Frank Miller described an encryption method that could not be defeated - the One Time Pad. This included a pad book of random information that could use a single operator to encrypt the information, character by character, using that pad book of random information. Each random character could only be used "one time". The receiver would have an identical version of this pad book and, when received, would use the inverse operator to reverse the process one character at a time. If it was intercepted, there would be no way to figure out what the real data was without the padbook. The proof is a pre-algebra trick question X + Y = 10 where X represents the wire transfer and Y represents random numbers from the pad book. We have no way to solve for X or Y if both are unknown. Taking negative numbers into account, they really could be any integer. This is, clearly, an uncrackable encryption method.

Computer scientists have long sought a way to implement the One Time Pad in a network. With today's robust, high-speed telecommunication backbones powered by cheap, blazingly fast chips, abundant entropy, and a glut of storage for virtual pad books, computers can efficiently process One Time Pad encryption with the lowest possible latency.

The biggest challenge is the Key Exchange Problem. That is, how to conceal the pad's entropy/randomness from interception, recording, and decryption.

Stealth Networking

SmokeNet solves the interception problem through "hiding" the data during transmission by applying Moving Target Defense - an age-old method to conceal military assets - to high-speed networking. Instead of using a known port (such as port 80), SmokeNet constantly switches the port, thereby removing a key piece of information required for interception. Red Team test results, requested by the US Air Force CyberWorx, and conducted by Viasat, an independent 3rd party, found a breath-taking ZERO vulnerabilities. That was the first time that feat had been witnessed. In fact, the testers were not even able to find the network devices were transmitting data. SmokeNet not only hid the data during transmission, it also hid the edges of the network. SmokeNet, essentially, created a virtual network smoke screen. If the network can not be seen, the

data can not be intercepted. This is truly impressive given that routers are designed for data interception.

The network data in motion is now effectively stealth as it is hidden from all adversaries. This stealth capability also applies to the network server as it does not have any identifiable ports open while SmokeNet is being used. This means the server will look like a laptop in a coffee shop.

Future Proof

As technology moves forward, new and more sophisticated threats are emerging. These threats will make the industry's already porous cybersecurity even less secure. Relatively sophisticated attackers will harness advances in computing to break in, without the need for social engineering. New hacks and cracks will happen in compute time.

Quantum Computing

The threat drawing the most attention is Quantum Computing. If this reaches its desired potential, it will be able to crack most encryption in near real time. In 2014, a project was started to create a new encryption standard that would be "resistant" to Quantum Computer cracking. Like with prior standard encryption, it was not necessarily designed to be secure. It was born out of a world of Cyber Offense. The "post quantum" encryption is actually turning out to be less secure than its predecessors. The crack that was most disturbing reveals the next threat - AI.

Artificial Intelligence

During Testing of post quantum encryption by the KTH Royal Institute of Technology, Stockholm, Sweden, researchers discovered a way to defeat one of the top 4 quantum resistant encryption techniques, CRYSTALS-Kyber, using AI. The AI not only proved the encryption was not secure, it also revealed the threat of AI. The AI used, recursive learning, was relatively primitive yet effective. The problem with this kind of capability is it can derive a proof with no training or aptitude. If this kind of algorithm makes it to Open Source or the Dark Web, it allows anyone to crack encryption.

SmokeNet Solves Both Problems

SmokeNet is born from stealth and uncrackable encryption. These two factors make SmokeNet impervious. Even these future threats are no match for uncrackable encryption and stealth network technology. The key to this is the use of true randomness. True random has no way to be discovered or derived. We use true random for: 1) encryption as "pad" or "key" material and 2) our movement in the network leaving the next change unpredictable.

Neither a Quantum Computer nor Artificial Intelligence can defeat randomness. In the case of a Quantum Computer, even it can not solve an unsolvable problem like the One Time Pad. In the case of AI, because the movement in the network is random and unpredictable, there is nothing for it to solve for either. AI also has no proof to derive because the math is too simple and, again, unsolvable.

Easy Install

SmokeNet runs on separate hardware and not in software, making it truly secure. This is the prescribed method in Zero Trust Architecture. By running on its own hardware, SmokeNet blanketly removes all potential Operating System and device vulnerabilities including those compromised by Cyber Offense backdoors.

Moreover, with the exception of maybe connecting to a wifi network, all SmokeNet devices are plug and play. A SmokeNet device is easy to set up as a private network, SmokeNet WiFi network, or small USB connected device protecting an individual computer. The network inside the tunnel runs under the same standards as the Internet. Designed to be simple to operate, SmokeNet works with little to no extra effort. All of the complexity is hidden so staff does not require much in the way of specific detailed, technical training.

Department of Commerce Approved

SmokeNet is approved for sale commercially by the Department of Commerce. The approval included a comprehensive NSA review of the security and encryption. That review is extremely favorable. NIST, the group that runs the encryption standards, is under the Department of Commerce. In other words, the highest levels of US cybersecurity have given SmokeNet their seal of approval. Export of SmokeNet is restricted to friendly nations which speaks volumes to how powerful the NSA believes this security measure is.

Customers can purchase SmokeNet with peace of mind that it is approved for use and has been thoroughly vetted.

Summary

The cybersecurity problems we see on the Internet today border on the absurd. With Cloud Computing, work from anywhere policies, video conferencing, … companies and corporations are continuing to embrace the Internet. At the same time, companies are increasing their exposure to cyber attacks.

SmokeNet sends your private company data through a network tunnel that makes your data stealth. By hiding the data, SmokeNet can utilize the only known uncrackable encryption - the One Time Pad - making it impervious to decryption.

The Department of Commerce has approved SmokeNet for sale and export to a limited number of approved countries. It is so powerful they do not want the technology in the wrong hands. NSA's review validates SmokeNet's encryption and cybersecurity methods, effectively certifying them for use by a corporate world that is constantly under cyberattack by increasingly sophisticated cyber criminals and bad actors.

When your company decides to implement SmokeNet, it uses the same network standards used for the Internet. SmokeNet is, for the most part, plug and play. The implementation is in hardware, not software, removing it from being exposed to any potential device breaches or backdoors.

Move towards Zero Trust Architecture with a simple, clean, approved solution - SmokeNet.