International Research Journal of Engineering Science, Technology and Innovation Vol. 7(4) pp. 10, August, 2021
Available online https://www.interesjournals.org/engineering-science-technologyinnovation.html

Theory

Constructing a Network Defense Paradigm The Third Zone Network Architecture (3ZAM)

Anthony Mazza*

University of the District of Columbia, Washington, DC USA

E-mail: anthony.mazza@udc.edu

Abstract

Network protection strategies are in a continued state of refinement, with "defense in depth" the lingering buzz phrase for the industry- a concept of adding security protection at multiple layers rather than relying only on a perimeter firewall. But there are major issues associated with current networking architecture and best-practice DMZ models. Even with an alleged 98.5% security effectiveness when deploying best-of-breed Intrusion Prevention System (IPS) products (factoring in exploit block rates, anti-evasion capabilities, etc.) and Next-Generation Firewalls (NGFWs), network attacks that slip past one security product are likely to slip past another. This paper explores a new network defense paradigm that incorporates Zero Trust Architecture within a Third Zone Architecture Model (3ZAM). 3ZAM recognizes network security as a "process response" to the Lockheed Martin Cyber Kill Chain® model and instantiates emerging trends in software-defined perimeters (SDPs), pseudo-appliance strategies, micro-segmentation, and Virtual Private Networking (VPN) alternatives.

Keywords: network security, DMZ, Cyber Kill Chain®, SDP, VPN, VLAN.

INTRODUCTION

Information and Communication Technology (ICT) infrastructure has advanced significantly over the past 20 years, spawning a surge in the need for communication and collaboration capabilities. Computer devices and software applications leverage this infrastructure to produce solutions in varying degrees of innovation. The ever-increasing volume of computer devices, software applications, and data crossing between many different networks depend on this ICT infrastructure. Network protection strategies are in a continued state of refinement, with "defense in depth" the lingering buzz phrase for the industry- a concept of adding security protection at multiple layers rather than relying only on a perimeter firewall [1].

Unfortunately, many issues conspire to thwart ICT's ability to keep pace. Skill sets, budgets, and legacy systems hinder investment. Fundamental network architecture has not substantively changed-firewalls remain the principal defense mechanism and have been used to separate computer networks since the Internet first emerged. Two issues emerge limitations on communication and security design flaws. network attacks that slip past one security product are likely to slip past another [2]

Firewalls inherently introduce trade-offs between spectrums of security versus collaborative capabilities. Only a fraction of the collaborative capabilities inherent in the Internet paradigm is realized because they are predicated upon single dimension architectures. Also, traditional network architecture does not effectively separate and protect private networks (and the assets within) from all other networks. Adversaries continue to exploit this ICT design flaw; a proliferation of sophisticated network attacks have led to the single greatest period of wealth transfer in human history- all illegally via credit card fraud, intellectual property theft, and costs associated with malicious attacks. The proliferation of attacks and their growing sophistication translates to an accumulating advantage over increasingly distressed computer networks. As a result, the potential for cyber-crime and/or computer network invasion are among the greatest risks facing governments and businesses.

Incorporating a "process response" to the Lockheed Martin Cyber Kill Chain® model [3] and incorporating

Software-Defined Perimeters (SDPs) and VPN-alternatives is a relatively simple and inexpensive change in computer network architecture. It will substantially improve cyber security and significantly enhance collaborative capabilities.

NETWORK SECURITY ARCHITECTURE ISSUES

Topology

Network Architecture and the strategies employed to protect it vary significantly by company, geography, policy, and budget. Networks tend to be deployed in either a traditional architectural framework or a "best-practices" DMZ structure. The U.S. Computer Emergency Response Team (US Cert) has directed that network services requiring public access should only be deployed within an organization's DMZ to prevent public access to an organization's internal trusted network [4]. Both of these approaches expose internal servers, rely on firewalls and VPN, and are inherently flawed facilitating several vulnerabilities.

DMZs

When implementing a "best practice" DMZ, an organization's publicly accessible servers (e.g. web, email, file management) are "moved" from the internal private network and into the DMZ. These services are made accessible from external networks. Nodes on the internal private network can access the DMZ via an internal firewall and possible authorization processes. Access to the internal systems is typically limited only to nodes on the same private network. Even though a security zone has been established for nodes on the internal private network, this architecture exposes some of an organization's prime business servers directly to potentially dangerous external networks. Proxy, gateways, or bridging services can be implemented to serve client requests on behalf of the internal servers; but remote clients communicate with servers in the DMZ and these servers have the required access credentials to access the servers in the organization's internal private network through the internal firewalls. Moreover, due to the cost and complexity associated with the effort, DMZs are inconsistently deployed across enterprises and are fundamentally and paradoxically dependent upon VPN. They are expensive to install, maintain and service in production. A common problem for large organizations with fragmented and distributed networks (i.e. numerous networks internally and externally) is the perceived level of "trust" between these networks. Therefore, DMZ security is typically reserved only for Internet connectivity.

Virtual Private Networking (VPN)

Virtual Private Networking (VPN) is a fundamental precept of traditional and DMZ network security deployments. Establishing virtual point-to-point connections through virtual tunneling protocols and data traffic encryption creates a VPN. VPN enables a device to send and receive data across shared or public networks as if it is directly connected to the private network. The concept of VPN is to enable remote users to benefit from the functionality, security, and management policies of the private network.

VPN poses a significant problem to providing both a layered security strategy and contributing to a defense-in-depth solution. The default topology of a VPN often exposes the entire network or security zone where the VPN Server resides, because the specific purpose of a VPN is to provide access to such an entire network [5]. To properly implement VPN into a layered strategy, the VPN server should be isolated into its security zone with clients being allocated addresses within that network. Isolating the VPN service requires additional complex network routing and firewall rules before VPN clients can reach appropriate resources. VPNs are often used because the nodes in the DMZ are unable to directly reach the servers in the internal private networks or have controlled, restricted access for certain services only. The problem is that VPN bypasses the DMZ security zone and allows traffic to flow from the remote VPN client to the private networks unrestricted (by default).

In an attempt to mitigate "services exposure" or sidestep the costs involved with a DMZ deployment, many companies have begun to deploy Router-based DMZ Host Options. A router-based DMZ option represents a "redirect-all" to a designated machine on the private network. This machine is assumed to be "hardened" and capable of handling any traffic directed to it -valid and malicious alike. This type of machine is often referred to as a Bastion Host [6].

A Bastion Host port on a router supports a router's fundamental inability to support every possible protocol requiring specific handling to a designated server. For the router to handle redirection of an unusual protocol (e.g. GRE), it simply redirects all unspecified redirections to a designated, hardened server. With the "DMZ Host" option enabled, unspecified traffic is routed through to the IP address of the Bastion Host, effectively operating as a firewall. The Bastion Host must be configured to filter unwanted traffic and correctly handle valid traffic on behalf of other servers or nodes on the network. The network administrator must still perform the required "hardening" of this designated server and integrate the required services to handle anomalous requests. This strategy does not negate the act that servers are typically directly connected to the same internal network they are designed to protect. If this dedicated server is breached, the likelihood of a breach affecting the remainder of the network is elevated.

Note that the use of the term "DMZ Host" is a misnomer: router manufacturers market an inappropriate use of the term "DMZ" within their products suggesting that consumers may rely upon their use to implement a DMZ-based security solution. This is not a safe option and results in compromising the overall security policy.

Firewalls

The typical Computer Network Security Architecture

is predicated upon protecting an internal network. Therefore, when an organization's "private" network and affiliated computer devices are connected to the Internet, fundamentally they are directly linked to millions of other computer networks and devices. In internal networks, switches are used to link network segments or devices. This direct connectivity has many associated risks. As a result, firewalls are often internally deployed in larger organizations with highly fragmented and widely distributed networks.

Firewalls can be classified as a "network membrane"-a permeable barrier allowing both good and harmful packets of data to pass through too or out from computer endpoints at some stage. Firewall components to try and control the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on a "predetermined rule set". Most firewalls can perform basic routing functions to forward data packets between computer networks.

This attempt to establish some form of separation between network segments increases cost and complexity. It also inherits potential risk due to poor configuration and/or weaknesses associated with firewalls and other security products [7]. For example, a "port opening" is often created in the network by establishing a niche rule at the firewall to "allow TCP port 443 (HTTPS) any to any". This allows "superficially secure" connections to be established. Even in instances where a remote access gateway is deployed to strengthen security protocols, this open port is generated the instant an internal computer in a network communicates directly with an external service without authorization, authentication, and/or proxy services.

A Next-Generation Firewall (NGFW) is evolved firewall technology, combining traditional and other network device filtering functions, such as Deep Packet Inspection (DPI), an Intrusion Prevention System (IPS), VPN connections, TLS/SSL encrypted traffic inspection, website filtering, QoS/bandwidth management, antivirus inspection, and third-party identity management integration (i.e. Active Directory) [8].

The effectiveness of different firewalls' IPS engines varies significantly, with "effectiveness" ranging from 90% effective in addressing vulnerabilities, exploits, and evasion techniques, to scores as low as 25%. Some firewalls also offer a poor cost per protected data element, and many have an unacceptable impact on network performance [9].

Network firewalls protect the network traffic; Web Application Firewalls (WAFs) protect the app. A WAF operates through policies that protect against vulnerabilities in the application by filtering out malicious traffic. They analyze and filter all HTTP requests to a web application and block requests identified as malicious. WAFs typically offer simpler ways to enact policy modifications, allowing for faster response to varying attack vectors [10].

To separate malicious requests from legitimate ones, a WAF analyzes the different parts of a web resource request- the headers, parameters, and body of the query, etc. They attempt to identify patterns that match with an attack. Unfortunately, false positives are typical for WAFs. These are legitimate requests that are blocked for some reason, so an application stops working.

Too often, WAFs generate "a false sense of security among developers, system administrators, and staff that are responsible for the security of companies and organizations. Security protocols are neglected and preventive measures such as code and infrastructure audits are not taken because of the use of a WAF" [11].

Like any other application, if a WAF has vulnerabilities, it fails. This is a particular problem with open-source WAFs. For example, Nginx is used as one of the most widespread solutions for the implementation of WAF through different scripts written in LUA. System Administrators neglect to account that the module responsible for the integration of LUA in Nginx (Lua-Nginx-module) does not allow access to all the information of a request. "This means that no matter how effective a WAF is in detecting attacks, there is certain data that is invisible to its analysis. If the parameters that contain malicious data are outside the scope to which the WAF has access, it will be unusable" [12].

Despite the shortcomings of both, using an NGFW and a WAF together provides broader security coverage. A network firewall will address an attack at the edge of the network by blocking incoming malicious traffic; the WAF will stop specific layer 7 attacks against the application, whether an attempt to exploit vulnerable code-level or software libraries via deserialization or injection attacks or a DDoS attack focusing on the compute resources of the application.

Encryption

Encryption is the data manipulation strategy for messages or files to be made unreadable, ensuring that only authorized access to that data. Using complex algorithms, a key provided by the message sender is used to scramble and decrypts the same data. Encryption attempts to ensure that information stays private and confidential, "at rest" or in transit.

Encryption technology comes in many forms, with key size and strength generally being the most significant differences in types. Historically, the Data Encryption Standard (DES) was the de facto industry standard until "Triple DES"-which used three sets of encryption keys was introduced [13]. The Advanced Encryption Standard (AES) [14] superseded triple DES. AES is used to secure wireless computer networks, WAP and eventually WiFi Protected Access 2 (WPA2) [15].

Encryption is critical in securing client-server sessions, but it cannot differentiate between legitimate users and attackers. It also introduces a problem for active traffic inspection tools because of the encrypted information. As a result, Secure

Socket Layer (SSL) intercept features are also needed in conjunction with Application Delivery Controllers (ADCs) for deep packet inspection. Together, these strategies prevent an In/Out bound relay of malicious activity. SSL and TLS (Transport Layer Security) allow for transport-layer security via public-key encryption and are typically employed over HTTP, FTP, and other Application- layer protocols. HTTPS (HTTP over SSL) is the primary remote access technology used for e-commerce, credit card validation, and other transaction websites.

The most endemic cryptographic system, Public-key cryptography, (also known as asymmetric cryptography) uses two different but mathematically linked keys one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret [16].

In another widely used asymmetric algorithm, RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. Many protocols like a secure shell, OpenPGP, S/MIME, and SSL/TLS rely on RSA for encryption and digital signature functions. RSA signature verification is one of the most commonly performed operations in network-connected systems [17].

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network [18]. SSH is generally used to access Unix-like operating systems. It provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. The protocol specification distinguishes between two major versions: SSH-1 and SSH-2. The standard TCP port for SSH is 22 [19].

SSH vulnerabilities are the subject of an ongoing debate, where some experts allege that the National Security Agency may be able to decrypt SSH traffic. A later study asserted that the SSH protocol itself was not compromised [20].

Encryption strategies are only as good as the underlying software or implementation methods employed. For example, between 2014-2017, OpenSSL was used by approximately 66% of all active websites on the Internet. Particularly vulnerable, an OpenSSL attack known as Heartbleed (formally “CVE-2014-0160”) allowed a potential attacker to read up to 64 kilobytes of memory per attack on any connected client or server [21]. Seven years later, OpenSSL is used by less than 10% of all active websites [22]. OpenSSL version 3.0.0 was released in September 2021 [23].

Quantum computing poses the greatest threat to encryption strategies. Utilizing properties of quantum mechanics Quantum computing processes large amounts of data simultaneously, achieving computing speeds thousands of times faster than today's supercomputers [24]. Quantum computing can factor decryption algorithms to in the same amount of time it takes for normal computers to generate encryption keys. This would make all data protected by current public-key encryption vulnerable to quantum computing attacks. Other encryption techniques like elliptic curve cryptography and symmetric key encryption are also vulnerable to quantum computing [25].

SSL VPNs

SSL-based Virtual Private Networks (VPNs) provide remote-access connectivity from virtually all Internet-enabled locations by using a Web browser and native SSL encryption. It typically does not require special client software to be pre-installed on the system SSL; VPN connections are dynamically downloaded on an “as-needed” basis. All VPN traffic is transmitted and delivered through a standard Web browser, so only Web-enabled applications can be accessed using a clientless connection. SSL VPN full network access is delivered through a lightweight VPN client that is dynamically downloaded. Over the past 18 months, high-profile corporate attacks illustrate the impact of inadvertent free-flowing information on malicious entities.

VPN breaches resulted from security flaws. SSL VPNs use Internet browsers as clients (unlike IPsec-VPNs, which use dedicated clients). Each browser has its unique security flaws, meaning that SSL VPNs have inherently weak clients. A hacker can exploit these browser vulnerabilities to spoof a certificate authority (CA) used in the SSL VPN verification process. The integrity of the SSL certification process is also problematic because the certificate authority entities are not organized or regulated.

Recently, seven VPN providers left 1.2 terabytes of private user data exposed. These companies claim that they do not keep logs of user online activities. The exposed data, found on a server shared by the services, included the Personally Identifiable Information (PII) of potentially as many as 20 million VPN users [26]. In a separate and later incident, more than 21 million mobile VPN app users had credentials stolen including email addresses, randomly generated password strings, payment information, and device IDs belonging to users of three VPN apps-SuperVPN, GeckoVPN, and ChatVPN [27].

NETWORK VULNERABILITIES

A network “vulnerability” is a software, hardware, or protocol weakness that may provide an attacker the ability to gain unauthorized access to a network asset (i.e., improperly written code that allows for exploitation via a buffer overflow attack; an active network port in a public area that presents the opportunity for physical network access; improperly devised authentication systems; etc.). Humans are frequently a source of vulnerability [28].

Adversaries search for holes in routers, firewalls, switches, software, end-point devices, and momentary lapses in user behavior to breach network defenses. Once exploited, network lapses enable the attacker to gain unauthorized and often undetected access to target networks, where

they can redirect traffic on a network or intercept and/or alter information while in transmission [29]. As a result, adversaries can gain sensitive data, disrupt network performance, alter important information, attack other trusted systems on the network, and/or launch attacks against other networks. Common network threats include all types of viruses, worms, and other malware/hardware and application-layer attacks; "man-in-the-middle" attacks; spoofing and identity spoofing; phishing and sniffers; DDoS and brute force attacks; ram scraping; ransomware; etc.

Advanced Persistent Threats (APTs) are skilled, well-resourced multi-episodic intrusion campaigns targeting highly sensitive economic, proprietary, or national security information [30]. APTs accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms.

The introduction of mobile devices and the exponential explosion of usage ushered in a new driver of threats: end-user and client-side devices. Advanced threats such as botnets, malicious active content, cross-site scripting, unknown vulnerabilities on external hardware and client-side devices can now bypass perimeter network security appliances. Poorly crafted mobility applications cause significant problems, especially when they communicate directly with primary network systems. Problems are compounded when users directly connect (i.e. via network switches and wireless access points) portable and "Bring Your Own Devices" (BYOD) to an organization's internal network and the hazards they contain after touching many different and potentially dangerous external networks.

The market is experiencing a mass migration to virtualized infrastructure in cloud environments. The commercial benefits of cloud infrastructure are well documented: reduced costs, streamlined administration, and improved flexibility. However, moving data and resources to a cloud model introduces additional security issues. Supply chain viability (the weakest link in the cloud infrastructure model is often an under-financed or mismanaged corporate provider), vendor-specific protocols, and the common practice of providing low-level engineers and administrators with extraordinary access levels create significant vulnerabilities in cloud infrastructure deployments [31].

NETWORK DEFENSE APPROACHES

Defense in Depth

A recent trend in traditional and DMZ network security is the adoption of a "layered security" design, where multiple mitigating security controls are combined in a manner intended to increase the protection of assets (i.e., authentication, encryption, fraud detection, remote access protocols, etc.). The philosophy behind a layered security defense is a "bend but don't break" tactic to resist rapid intruder network penetration by interposing resources that are intelligently deployed or consumed in a manner to slow incursions, and not be exhausted in the process. Layered security is essentially a delaying tactic, enabling the time to marshal appropriate responses to malicious activities. It gave rise to the notion of the "defense in depth" strategy, a militaristic euphemism that involves the deployment of technical security tools, imposition of security policies, operations planning, user training, physical security, and information assurance personnel involvement [32].

Software-Defined Perimeters

The Cloud Security Alliance (CSA) purposively conceived the software-defined perimeter (SDP) security framework to protect application infrastructure from the network-based attacks. SDP incorporates security standards from the National Institute of Standards and Technology (NIST) and security concepts from the U.S. Department of Defense (DoD) into an integrated framework.

SDPs provide the ability to deploy perimeters that retain the traditional model's value of invisibility and inaccessibility to "outsiders," but can be deployed on the Internet, in the cloud, at a hosting center, or on a private corporate network. It incorporates standard security tools (i.e., PKI, TLS, IPsec, SAML) and concepts (federation, device attestation, and geo-location). SDP connectivity is based on a "need-to-know" model, in which device and identity are verified before access to the application infrastructure is granted. Application infrastructure is effectively "black": the infrastructure cannot be detected because there is no visible DNS information or IP addresses. SDP mitigates the most common network-based attacks, including server scanning, denial of service, SQL injection, OS & application vulnerability exploits, password cracking, man-in-the-middle, cross-site scripting (XSS), Cross-Site Request Forgery (CSRF), pass-the-hash, pass-the-ticket, and many others (see NIST, SANS, and more). SDP uses a lightweight access protocol to support deployment on mobile applications, networked sensors, and application servers as its end-point strategy.

The SDP architecture consists of two components: SDP Hosts and SDP Controllers. SDP Hosts can either initiate or accept connections. These actions are managed by interactions with the SDP Controllers via a secure control channel established through "mutual VPNs". The control plane is separated from the data plane to enable extensibility [33].

The current industry hype surrounding SDP is as much a reaction to the actual product functionality, as it is a hopeful expectation of a long-sought solution. The ability to provision a network of services at the perimeter using software to protect the internal network is a major step forward. On the flip side, the provisioning of services on the perimeter creates additional endpoints needed to execute service requests (in/outbound). The fact that the SDP design depends upon mutual VPN connections is also a potentially significant concern, which will require an alternative strategy to protect and hide perimeter network links.

Cyber Kill Chain Modeled Response

Lockheed Martin's Computer Incident Response Team created a network defense process based upon advanced persistent threats: the Cyber Kill Chain® (Figure 1).

This process was designed as an intelligence-driven network defense strategy and it identifies the seven steps taken by master hackers to infiltrate a network: reconnaissance; weaponization; delivery; exploitation; installation; command and control; and, actions on objectives.

The cyber kill chain was intended to influence actionable responses, and align enterprise defensive capabilities to the specific adversarial processes.

Lockheed Martin experts also prescribe a course of action matrix using the actions of detect, deny, disrupt, degrade, deceive, and destroy from DoD information operations (IO) doctrine (U.S. Department of Defense, 2006) [34]. Borrowing from this approach, the Third Zone Network Architecture (3ZAM) can be constructed in a manner calculated to address prevailing and prevalent network attacks. See Table 1 below:

Figure 1: Lockheed Martin's Cyber Kill Chain®.

Intrusion Detection Strategies

An often-neglected element of the typical DMZ-like network strategy is the failure to implement seemingly redundant Intrusion Detection Systems (IDS) and Security Incident Event Management (SIEM). As critical as it is to segment the network into different zones, it is equally important to monitor the DMZ for potential breaches in the security deployment [35]. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to continually improve network defenses [36]. (See, E. Data Collection: Surveillance through Deception, below.)

The successful DMZ monitoring process would rely heavily on heuristic analysis of network traffic using special sensors designed to work in a promiscuous mode allowing the sensor to pick up all network traffic for analysis. Events occurring on the network would be delivered to a central data collection server for further analysis and "action protocols". Given the nature of this analysis, this process is prone to initiating false positives, which then require intensive and costly manual intervention to ascertain.

An alternative to this network-level monitoring is host-level intrusion detection. The theory is the same software is loaded into a given host and monitors the host for unexpected changes and reports them either directly or to a central server to raise the alarm on behalf of the host. This type of detection is less prone to false positives due to the physical, non-fragmented nature of the monitoring. Host-level IDS monitor elements of the host (most often the file system) for changes to files or folders it considers severe

Table 1. Sample 3zam cyber kill chain response.

Response Attack Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Behavioral analytics network security monitoring (NSM)	Close Endpoints	Access Control Logs	Blacklist	Detector IPs	Disable botnet Network Configuration
Weaponization	NSMNetwork Intrusion Detection Systems (NIDS)	Network Intrusion Prevention Systems (IPS) Containers	Multiple DNS Tracing analysis AV	Call Home Counter-attacks	Honeypots	Counterflood Techniques
Delivery	NGFW Proxy filters NSM	NGFW Close Endpoints 3ZAM	Multi-factored Authentication (MFA)	Hypervisor	Plug-in Authentication Header	IPSec attack Call Home Counter-attacks
Exploitation	NIDS NSM	Patch NGFW 3ZAM Containers	Data Extraction Prevention (DEP) AV	Packet filtering	Dummy files Dispersal	IPSec attack Call Home Counter-attacks
Installation	NIDS NSM	ch_root jailing MFA 3ZAM Containers	Hypervisor AV	Stratify internal networks	Honeypot Tarpit	IPSec attack Call Home Counter-attacks
Command & control	NIDS NSM	Packet filtering MFA 3 ZAM	Hypervisor	Stratify internal networks	DNS redirect	IPSec attack Call Home Counter-attacks
Reconnaissance	Security Policy	Close endpoints 3ZAM	Hypervisor	File tracking	Honeypot	File Infections Alert authorities

enough to be a problem or a result of a breach. The drawback to host-level IDS is the need to implement software (instead of a physical sensor) onto every host within a security zone implementing an Intrusion Detection System. It might be possible to create a blend of the two types of IDS by placing physical sensors to monitor the network while host-level systems are implemented on more sensitive nodes.

The VPN Alternative in the Third Zone Architecture

Replacing VPN in the Third Zone Architecture requires new Peer-to-Peer technology implemented at the Data Link Layer (Layer 2 of the OSI model). Borrowing from the SDP protocol, this software establishes an entirely new virtual network (VN) over the top of existing physical networks using a mesh topology. Nodes within the VN can be disparate and located anywhere, so long as they can be reached over a common set of connections such as the Internet. Nodes can easily reside behind NAT firewalls because the UDP hole-punching methods of the VN software allow for direct communications over most commercially available firewalls.

The VLAN network created by the VN software would default to a closed network model where only those computers running a Peer client can communicate on the VLAN created between peers. If a machine is not running, even a Peer with correct credentials will not be aware of nor be able to communicate on the VLAN. This would leave the node isolated in its physical network (figure 2).

Servers in a Third Zone Network Platform are not part of the VLAN and therefore, the Third Network security zone is not exposed to any of the traffic flowing through the VLAN.Using the illustration in Figure 3,only one of the three computers in the trusted network is connected to the VLAN by running a peer with appropriate credentials to join. The other two nodes are unaware that the VLAN exists, as there are no routing table entries to make them aware of the VLAN. Also, any traffic generated on the VLAN is completely encrypted at the layer two OSI level.

The Broker Server responsible for assisting with direct P2P communications for the VLAN may reside either on the Internet itself or more safely in the Third Zone Network. This Broker Server never participates in any of the VLANs it assists in creating, and it never has access to the encryption keys needed to decipher the encrypted traffic.

Because an entirely new and closed virtual LAN is created, no part of the internal network is automatically extended out to a remote client in the way a VPN would. Only selected nodes in the private physical network can communicate on the VLAN. Personal packet filtering software is often available by default on most operating systems can be used to secure the node against unwanted incoming and/or outgoing traffic.

In essence, the VLAN functions as virtual “Internet over the top of the physical Internet”, but with the added benefit of creating a broadcast domain. From the closed network model implemented by default with VN software (the default P2P model), it is possible to begin replicating the facilities of VPN and providing access to physical networks for connected VN members. This is a selective process and would not require the configuration of the nodes on the VLAN.

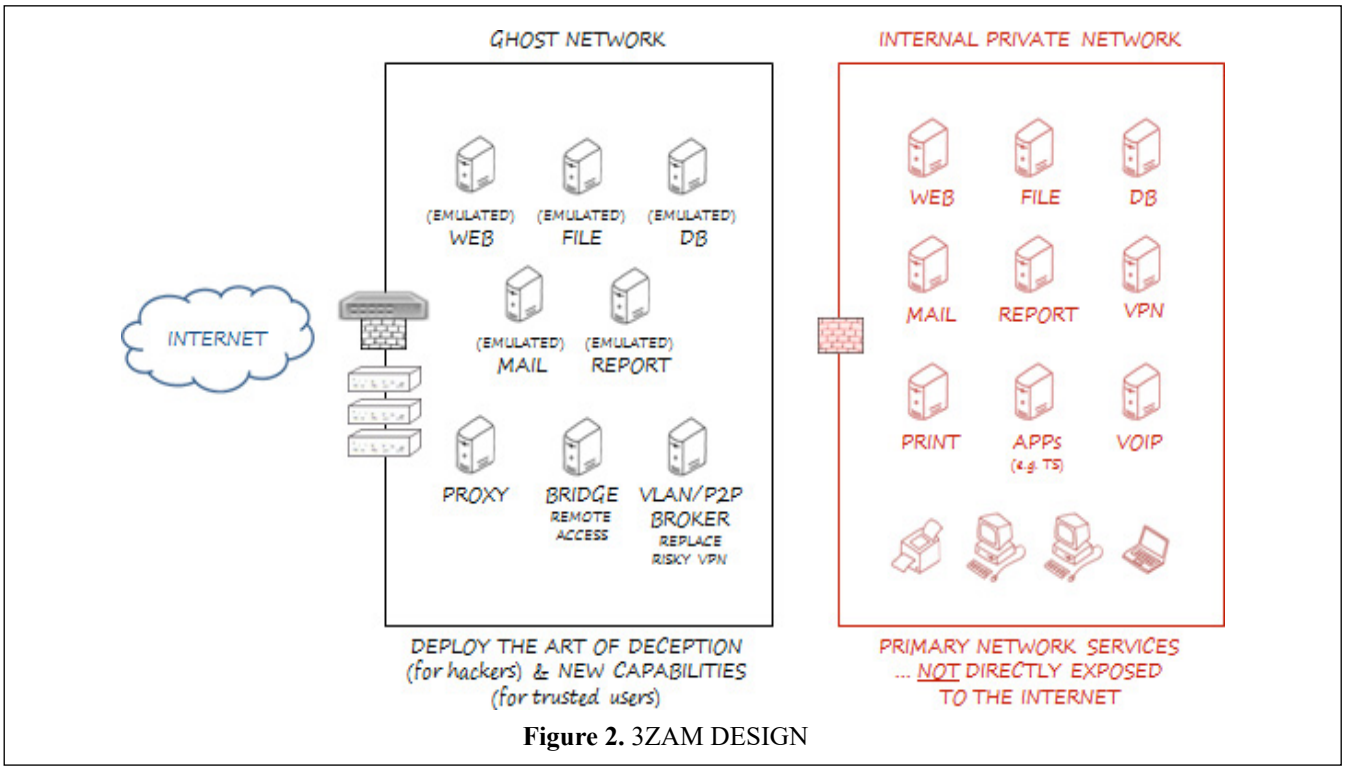

Figure 2. 3ZAM DESIGN

By enabling routing capabilities in a given Peer and with the addition of routing table entries to appropriate physical and virtual nodes, it is possible for a Peer to grant remote Peers access to the physical network of the local node. This model is called Peer-to-Network mode and emulates SSL VPN. Additionally, infrastructure VPN can be emulated by enabling routing in more than one Peer on the VLAN. With appropriate routing table entries applied, it is possible for one physical network to communicate with another physical network using a routing enabled Peer on each network.

While prudence must also be exercised in this model, the ability to create an encrypted tunnel between two trusted, physical networks would be extremely beneficial especially for medium to large organizations with an existing DMZ infrastructure. Moreover, unlike SSL encryption, VN requires prior key knowledge between trusted users that an attacker would not possess.

Zero Trust Elements in a Third Zone Platform

The "zero trusts" concept dates back at least a decade, yet the term is still evolving. Various approaches include the two (arguably) most successful: micro-segmentation (dividing data centers and cloud environments into zones) and software-defined network perimeters to endpoint agents or gateways.

The National Institute of Standards and Technology (NIST) published a zero-trust framework in August 2020. According to the NIST, the principles "are designed to prevent data breaches and limit internal lateral movement." The NIST describes zero trusts as a set of paradigms that "move network defenses from static, network-based perimeters to focus on users, assets, and resources." Whether internal or external, no connection is implicitly trusted and must be continuously authenticated and authorized before access to an IT resource is granted [37].

Since Covid-19 has ubiquitized the work-from-home paradigm, there is a renewed interest in the model. By definition, remote work naturally falls into zero-trust models because each user should have to strongly authenticate back to applications.

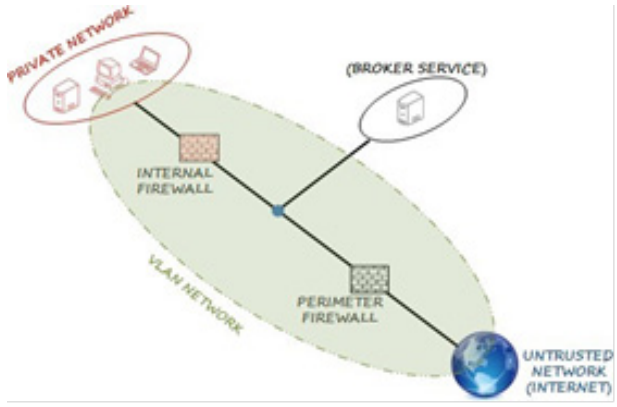

Figure 3. P2P VLAN

Security experts find that zero trusts is especially helpful within the context of the "cyber kill chain" framework. A zero-trust architecture includes both logical (policy engines, threat intelligence, and identity management, etc.) and infrastructure components (servers, routers, appliances, and other hardware). A zero-trust system needs to ensure that not only the user is authentic, but that the request is also valid [38].

For the process to work, risk-based, dynamic policies must be maintained for accessing the resource, and the zero-trust architecture would ensure these policies are consistently and correctly enforced. Ideally, the components (or modules) of the architecture are isolated from each other, and controls are maintained over a VLAN. Segmentation, continuous authentication, and Third Zone compartmentalization will effectively prevent intruder lateral movement inside a network.

Data Collection: Surveillance through Deception

The need for network defense strategies to develop, create and integrate proactive threat intelligence is more acute than ever, especially in critical infrastructure environments. One highly effective method of obtaining defense intelligence is through deception technologies. Deception technologies are defined by deceits and methods designed to thwart "an attacker's cognitive processes, disrupt an attacker's automation tools, delay an attacker's activities or disrupt breach progression" [39]. Deception capabilities typically create fake vulnerabilities in "assets" (systems and code), monitoring these assets for an attack is in progress, as a legitimate user should not see or try to access these resources. Cyber deception techniques are emerging in networking, applications, endpoints, and the data itself, with more complex systems combining multiple techniques [40].

In theory, Deception may provide analysts the ability to collect raw intelligence about threat actors as they reveal their Tools, Tactics, and Procedures (TTP). In practice, cyber defense in operational ICS is difficult as it often introduces an unacceptable risk of disruption to, or delay within, the critical systems (e.g: power grids). The hardware used in ICS is often expensive, making full-scale mock-up systems for testing and/or defense impractical. Much of the work that we see in today's literature is focused on creating Deception Environments in traditional IT enterprise environments.

Traditional Computer Network Defense paradigms have focused on reactionary measures, using tools such as signature-based detectors, white/black listing, IDS, etc. Event detection and correlation techniques are used to identify threats, which are then often handled manually, via obstruction-based responses (e.g., blocking). As threat sophistication grows, these perimeter-focused security

efforts will be rendered ineffective in combating competent adversaries [41].

CONCLUSION

The traditional computer network architecture model is becoming obsolete because BYOD and phishing attacks provide untrusted access inside the perimeter and SaaS and IaaS that change the location of the perimeter. New network architecture models must incorporate a "third zone" a Virtual Network of Services between an organization's primary network and all other networks internal and external. This small change in design will substantially improve cyber security and significantly enhances collaborative capabilities.

Implementing a layered security strategy is highly recommended due to its ability to "slow down" an attack on a private network. However, layered security often raises functionality and collaboration problems for remote users (e.g. employees) and stakeholders (e.g. suppliers, customers, joint venture partners). The cost and complexity of deploying a layered DMZ security strategy are beyond the capability of most SMEs. Organizations that can afford to implement layered DMZ security strategies, still face significant challenges with fragmented network segments and dealing with SMEs over the Internet. Adversaries often target SMEs because their networks are often easier to breach. Bot-Nets and keystroke logging are classic examples of this type of attack strategy where the smaller organization or user is not aware of their involvement in such an attack. In some cases, inadequate SME security enables tactics that are part of a stronger attack strategy focused against larger organizations. Larger organizations such as Fortune 500 companies, although having spent the time and money putting complex, defense-in-depth strategies in place, often face unknown vulnerabilities through attacks originating from breaches to smaller, less secured client networks. These smaller networks may have elevated and trusted access to the primary/larger network, making it the ideal conduit for the attack. Eventually, the larger organization's network is compromised- not as a result of their inability to implement strong security practices- but as a result of smaller entity clients being unable to do the same.

The IT market is inundated with a myriad of security products and best practices geared around traditional network architecture and principles. However, a far more strategic approach to network architecture is also needed – one that prevents the network breach from being initiated or contained post facto. By implementing advanced network architecture strategies- one which invites and incorporates many best-of-breed solutions- a significant benefit in security, productivity and collaboration can be realized.

Virtualizing the network into a single host (physical or virtual) eliminates risk and many costly aspects of applying a defense-in-depth strategy to network security (including cloud) and at the same time, provides a new platform from which business can deliver collaborative cloud services.

Micro-segmentation is a good start. Ensuring that only mission-critical and authenticated devices connect to the service access granted is a foundational element for 3ZAM that contemplates using a mechanism for distributing secure configurations to all multi-factored authenticated devices and ensuring the configurations are applied consistently.

There is also a growing industrial realization that a comprehensive, systematic, principle-based, modeling is more likely to produce long-term, lasting, reusable approaches for defensive cyber operations [42]. The proposed solution a Third Zone network architecture- adheres to principles applied in the physical world to protect assets and adopts and incorporates the most successful defense elements of DMZ and SDP solutions.

It improves upon the Enterprise Level Security (ELS) Model, which advocates the use of a DMZ layer and pseudo-appliances [43]. Instead, 3ZAM advocates the less expensive and easier to manage use of virtual services and VLAN technology. Virtual Services already obviate the need for pseudo-appliance to capture all of the inspection processes and places them into a single software process that resides in the application. This is the first step in realigning the priorities between the current approach and the end-to-end approach.

ACKNOWLEDGEMENT

Many thanks to Tim Gooch, who is the original architect and was instrumental in the development of this theory and paper.

REFERENCES

1. Snyder J, (2008) "Six Strategies for Defense in Depth: Securing the Network from the Inside Out," Opus One,. http://www.opus1.com/www/whitepapers/defense-in-depth.pdf

2. Blevins B (2014) "Research finds holes in the defense-in-depth security model," TechTarget.

3. http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

4. U.S.Cert, 2010. https://us-cert.cisa.gov/ics

5. Walker-Brown A (2013) "Managing VPNs in the mobile worker's world," Network Security, 1: 18-20.

6. Cole E (2011) Network security bible 768). 2nd Edition, John Wiley & Sons, USA.

7. Rahman M A, & Al-Shaer E (2013) "A formal approach for network security management based on qualitative risk analysis," Integrated Network Management, IFIP/IEEE International Symposium. 244-251.

8. Grier E (2011). Intro to Next Generation Firewalls. E-Security Planet.

9. McCormack C (2018). The problem with next-gen firewall protection. Sophos News. https://news.sophos.com/en-us/2018/01/01/the-problem-with-next-gen-firewall-protection/

10. Lutkevich B (2018). Web application Firewalls. TechTarget.

11. Farina D (2018). Serious Vulnerability in CloudFlare that Allows your WAF to be Disabled. Open Data Security.

12. The High Vulnerability With WAF- Open Data Security, 2018. https://opendatasecurity.co.uk/cloudflare-vulnerability-allows-waf-be-disabled/

13. Barker E. (2016). "NIST Special Publication 800-57: Recommendation for Key Management Part 1

14. NIST (2001). Announcing the AES Standard.: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

15. Jonsson J (2003). "On the Security of CTR + CBC-MAC". Selected Areas in Cryptography. Lecture Notes in Computer Science. 2595. 76-93

16. Stallings William (1990). Cryptography and Network Security: Principles and Practice. Prentice Hall. 165.

17. Cobb, M. (2018) RSA algorithm (Rivest-Shamir-Adleman). Tech Target. https://searchsecurity.techtarget.com/definition/RSA

18. Ylonen T, & Lonvick C. (2006). The Secure Shell (SSH) Protocol Architecture. Network Working Group of the IETF.

19. Network Working Group of the IETF, 2006, RFC 4252, The Secure Shell (SSH) Authentication Protocol.

20. Ylonen T. (2017). "BothanSpy & Gyrfalcon - Analysis of CIA hacking tools for SSH".

21. Frulinger, J. (2017). What is the Heartbleed bug, how does it work and how was it fixed?

22. trends.builtwith.com/Server/OpenSSL , https://www.internetlivestats.com/total-number-of-websites/

23. OpenSSL version 3.0.0 was released in September 2021

24. Grumbling E, Horowitz M (2018). Quantum Computing : Progress and Prospects. The National Academies of Sciences, Engineering, and Medicine (Washington, DC: National Academies Press. 1-5.

25. Quantum Computing and its Impact on Cryptography by Rob Stubbs on 29. April 2018.

26. Owaida A (2020). 7 VPN services leaked data of over 20 million users, says report.

27. Ruiz D (2021). 21 Million Free VPN Users' Data Exposed. Malware Bytes Lab.

28. Sanders C, and J. Smith (2013). "Applied Network Security Monitoring: Collection, Detection, and Analysis".

29. Acemoglu D, Malekian A, and Ozdaglar A (2013). "Network security and contagion," National Bureau of Economic Research (No. w19174).

30. Hutchins E. M, , Cloppert M. J, Amin R. M (2011). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, 2011.

31. MacDonald N, Young G, (2007). "Server Virtualization Can Break DMZ Security," Gartner Research, Inc., 2007.

32. E. Cole, "Network Security Bible."

33. Bilger B, Boehme A, Flores B, Schweitzer J, Islam J (2013) "Software Defined Perimeter," Cloud Security Alliance Working Group.

34. Hutchins, E.M.; Cloppert, M. , Rohan M. A. (2008). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". Lockheed Martin.

35. Chen Z, Han F, Cao J, Jiang X, S. Chen (2013) "Cloud computing-based forensic analysis for collaborative network security management system," Tsinghua Sci. Technol., 18: 40-50.

36. Bejtlich R (2013). "The Practice of Network Security Monitoring: Understanding Incident Detection and Response," No Starch Press.

37. NIST publishes Special Publication (SP) 800-207, "Zero Trust Architecture. https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207

38. Tollefson R, (2020). Using a Zero-Trust Model to Secure a Distributed, Remote Workforce. Transformative Technology.

39. Liang G, Weller J, Zhao F, Luoand Z, & Dong Y, (2017). "The2015 Ukraine Blackout: Implications for False Data Injection Attacks". IEEE Transactions on Power Systems. 32: 3317-3318.

40. Urias V, Stout W, Van Leeuwen B (2018). On the Feasibility of Generating Deception Environments in Industrial Control Systems. Sandia national Laboratories.

41. Stout W, Urias V (2017). Technologies to Enable Cyber Deception. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

42. Kott A. (2018). The significance of model-driven paradigms in cyber security: an introduction.

43. SimpsonW, Foltz K (2020). Network Defense in an End-to-End paradigm. The Institute for Defense Analyses (IDA), Alexandria, Virginia. https://aircconline.com/csit/papers/vol10/csit101414.pdf