SDP or VPN?

(Or both?)

This white paper describes the variety of issues that can arise when establishing a remote workforce. It compares the benefits of Safe-T's ZoneZero® SDP with generic enterprise VPN products and how sometimes, they can run in tandem for superior security results.

If you are a CISO, CTO, IT administrator or other personnel involved with IT security, this document is for you.

What's inside?

This paper covers how gradual steps toward a full SDP solution can help your organization's security needs. Items discussed include:

- ZoneZero SDP deployment options
- How to deploy Safe-T's Zero Trust Network Access (ZTNA) SDP solution inline or side-by-side with an existing corporate VPN
- How your enterprise can benefit from both SDP and VPN solutions

---

Soaring Number of Cyber Attacks

The number of high-impact devastating cybercrimes is increasing annually. Today's hackers use malicious software tools such as purchased or open-source malware to commit identity and financial theft, steal business data, and launch ransomware attacks.

A growing number of hackers operate as gangs using organizational structures similar to commercial businesses, and an increasing number of trained professional cybercriminals are sponsored by governments.

Example reports on hacking trends:

- RSA Conference, August 2021: "As we move into the third quarter of 2021, the trend is brutally obvious and increasingly alarming: Ransomware attacks are everywhere."
- Check Point Software, July 2021 "Mid-Year Security Report reveals a 29% increase in cyberattacks against organizations globally."
- Business Insider, June 2021: "Major Cyberattacks Are on the Rise in the US, Experts Say."

Traditional Enterprise VPNs

The main function of an enterprise virtual private network (VPN) is to enable end-users to perform their daily work remotely and securely. A VPN creates an encrypted tunnel through the Internet from a user's device to an internal corporate network.

The encrypted connection is designed to ensure that sensitive data is transmitted securely. The theory is, that unauthorized individuals will be prevented from eavesdropping on internal traffic. However, VPN software clients and servers are regularly breached by hackers.

The Rise of The Flexible Hybrid Remote Office

There has been a large surge in the number of employees working from home (WFH) instead of at their employer's physical office.

Many companies are discovering that an all remote, or partially remote hybrid workplace is a good idea. A hybrid office provides a win-win solution empowering both employers and employees.

Remote workers are usually more productive, more cost-effective, and far more scalable than a workforce required to commute to the office every day.

Newly hired millennials *expect* to be able to work remotely whenever and wherever they choose. The COVID-19 pandemic has also significantly contributed to the soaring rise in remote workers.

Many employees are locked down at home because of the COVID-19 pandemic. The result has been an unanticipated increase in remote users who need secure access to their organization's servers and applications.

"The COVID-19 pandemic brought about a huge experiment in widespread remote working. Business leaders are evaluating permanent remote working arrangements as a way to meet employee expectations and to build more resilient business operations."

*Source: Gartner

As the number of remote workers continues to increase, so hackers continue to attack remote WFH employees. Most organizations do not have enough administrators who know how to configure secure remote access. The lack of administrative personnel has created a dangerous VPN attack surface.

Remote Workers: Advantages

Remote workers provide their company many advantages. However, an organization must ensure user access is secure.

Enabling remote workers provides the following benefits:

- **Results:** Remote workers are more productive.
- **OPEX:** Remote workers are less costly. They do not require expensive office space. Additionally, employees save money on transportation, eating in restaurants, and having to purchase business clothes.
- **Health:** Remote workers who skip their daily commute to and from the office have been documented to be significantly more protected from exposure to the COVID-19 virus.
- **Stress:** Working remotely improves employee wellbeing by eliminating the stress of long daily commutes to the office.
- **Flexibility:** Increased versatility in choosing work hours promotes a better work-life balance.
- **Global reach:** New employees working remotely can be recruited from any geographical location.

Remote Workers: Company device use

A company can use different approaches for deploying end-user devices to remote workers. Each option provides advantages, costs, and security risks.

The company can purchase and issue a personal device to each employee, such as a laptop or tablet computer. However, before the user can work with the device, the company's help desk must provision and configure it. Steps required to do so include:

- **Adding** an appropriate company domain to the device
- **Mapping** necessary network drives
- **Activating** Windows Office apps.
- **Installing**:
    - Safe-T's SDP and/or a VPN Client (optional)
    - Antivirus software
    - Video conferencing software

Remote Workers: Own device use

Bring your own device (BYOD) is a trending company policy that enables employees, partners, and contractors to use their personal devices for work, either remotely or in the physical office.

BYOD is growing in popularity. As such, it is vital that IT personnel understand both its pros and its cons, in addition to knowing how to manage it securely within the organization. The main key challenge with BOYD is providing secure access on employee-owned personal devices.

BYOD Advantages

There are many benefits to enabling employees to use their own devices for work. Among them:

- **Cost:** Employers save the expense of buying company-owned devices such as laptops, tablets, and smartphones.

- **Time:** IT administrators do not have to spend valuable working hours redirecting responsibilities to end users. Additionally, the need to install software and patches is eliminated.
- **Convenience:** Users are far more comfortable using their own personal devices. This has been shown to lead to increased employee productivity.
- **One device for all:** Users can travel with a single device instead of carrying separate personal and company devices.
- **Work/life balance:** Employees can achieve an improved balance between their personal and professional lives.

BYOD: Remote work disadvantages

Increased security risks can arise when a company enables its employees to work remotely, or in-office, using their own devices. Among them:

- **Limited control:** The company does not own or manage the employee's device.
- **Data ownership:** The company may not own the company data stored on the employee's device, unless agreed by contract.
- **Compatibility:** The personal device may not support the company's choice of VPN.
- **Overly broad access:** Device owners are often granted overly broad permissions to connect with a VPN to the company's internal network.
- **Exposure risk:** Personal devices can cause increased security risks such as data leaks or infection by malware. The increased risks occur because the personal device is not managed by the company's IT department and the user might decide to share the device with a partner or family member.
- **Inability to wipe:** The ability to 'wipe' a hard drive may not be practical for some devices if personal and work data is not kept separated.

Enterprise VPN Challenges

VPNs were not designed for IT environments that span multiple data centers, require fine-grained end-user permissions, use public and on-premises clouds to host applications, and require the ability to scale up rapidly.

VPNs were invented when most traffic came from company owned devices connected to the corporate network. The company's network topology implemented a static perimeter that defined a separation between users inside and outside to the company's network.

Common VPN challenges include:

- **Overly broad access:** When a user logs into their VPN client, that user is considered 'trusted' and often has unrestricted network access. This overly broad access violates the best practices 'principle of least privilege'. With a Zero Trust model, such as Safe-T's SDP, no user is by default considered trusted.
- **No access segmentation:** Most VPNs cannot provide fine-grained network segmentation with varying levels of access for different types of users.
- **Lack of flexibility:** VPNs require constant management and cannot easily adjust to network changes.
- **Inability to scale:** VPNs make it complicated to scale up rapidly adding new users and network locations.
- **Non agnostic:** Most enterprise VPN clients cannot be installed on all devices and operating systems such as: MacOS, Chromebooks, and Android tablets.

Security Advisories: VPN vulnerabilities

There are many security advisories issued for VPNs. This is largely because hackers scan the internet for unpatched VPN servers and breach them by attacking open ports and known bug vulnerabilities. Hackers also steal login credentials using techniques such as email phishing and social engineering.

Reports on VPN Vulnerabilities:

- Attackers Heavily Targeting VPN Vulnerabilities, Dark Reading, April 21, 2021.
- According to Gartner, Inc research: By 2023, 60% of enterprises will phase out most of their remote access VPNs in favor of ZTNA.

Security Advisories for VPN Vulnerabilities:

The following VPN systems have recently disclosed vulnerabilities which resulted in security advisories being issued. The list includes VPNs developed by several well-known VPN companies.

*Advisory list source: SOCRadar, Inc.

Pulse Secure

CVE-2019-11510 Pulse Connect Secure (PCS): Pre-auth arbitrary file reading

CVE-2019-11539 Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS): Post-auth command injection

Fortinet

CVE-2018-13379 FortiOS: Pre-auth arbitrary file reading

CVE-2018-13382 FortiOS: Unauthenticated SSL VPN users password modification

CVE-2018-13383 FortiOS: SSL VPN buffer overrun when parsing javascript HREF content

Citrix NetScaler

CVE-2019-19781: Directory Path Traversal leads to RCE

Palo Alto Networks

CVE-2020-2050 PAN-OS: Authentication bypass vulnerability in GlobalProtect client certificate verification

CVE-2020-2005 PAN-OS: GlobalProtect clientless VPN session hijacking

CVE-2019-1579 PAN-OS: Remote Code Execution in GlobalProtect Portal/Gateway Interface

SonicWall

CVE-2020-5135 SONIC-OS: A buffer overflow vulnerability

CVE-2019-7481 SonicOS: Blind SQL injection vulnerability which can be exploited remotely

CVE-2019-7482 SonicOS: Execute arbitrary commands with nobody privileges on the device

CVE-2019-7483 SonicOS: Pre-authentication vulnerability

Cisco Systems

CVE-2020-3220 Cisco IOS: Cisco IOS XE software IPsec VPN denial of service vulnerability

Meeting The Challenges of Secure Remote Access

Safe-T's Zero Trust Network Access (ZTNA) solution implements a secure access paradigm that fundamentally does NOT trust internal or external employees by default.

There is no concept of a static perimeter.

The ZTNA architecture, also known as a software-defined perimeter (SDP), was developed in 2010 by a Forrester analyst. Since then, it has evolved to become the gold standard for cybersecurity in enterprises.

Heres' why:

- **Security and compliance:** Safe-T's ZoneZero SDP solution provides technologies that can help your organization achieve both effective security and IT regulatory compliance.
- **Transparency and seamlessness**: Safe-T's transparent deployment provides an innovative and unique network-centric ability to implement an SDP within corporate network VPNs, firewalls, and application services. Safe-T's SDP allows seamless integration across legacy infrastructure and authentication services.
- **No assumption of trust:** If a user is located on the LAN there is no assumption of trust. Safe-T's SDP denies trust by default and incrementally opens access to users while evaluating risk. Access is granted on a "need-to-know" least-privileged basis defined by granular policies.
- **Application-level access:** Safe-T's SDP approach provides users secure connections to back-end applications without placing the user on the network and without exposing back-end applications to the internet.

- **Authorized visibility only:** Users only have visibility to the backend services they are permitted to use. Backend services not authorized to a specific user are hidden. Hackers cannot breach what is not visible.

ZoneZero SDP Deployment Options

Deploying Safe-T ZoneZero is as easy as one, two, three:

1. **Choose**
   Select your preferred deployment method:

   - Public cloud
   - Private cloud
   - On-premises cloud
   - Hybrid cloud

2. **Deploy**

   Deploy three nodes on VMWare or Hyper-V infrastructure via our Dep VM images:

   - ZoneZero Authentication Gateway: Deployed in a cloud infrastructure or in a DMZ.
   - ZoneZero Access Gateway: Deployed in the DMZ.
   - ZoneZero Access Controller: Deployed in a corporate LAN.

3. **Configure**
   Once the VMs are deployed into your virtual environment, simply configure the nodes. For details, consult the *Safe-T® Data ZoneZero Administrator's Guide*.

ZoneZero SDP

ZoneZero transforms the way organizations grant secure access to remote users. By uniquely separating the authentication layer from the access layer, application-layer access is granted to authenticated users only. As a result, access-granted users are only able to connect to applications and services according to their identity. This greatly reduces the chances of lateral movement which in turn, mitigates risk. With SDP Concepts for ZoneZero, organizations can implement Zero Trust Network Access while at the same time providing secure and transparent access to any internal application, service, or data source either in parallel to, or instead of, an existing VPN.

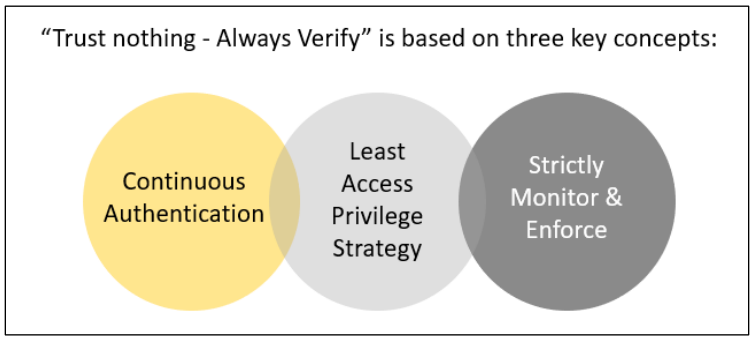
Least-privilege access: Only grants access to business applications and resources, per individual user, per authorized task.

Micro-segmentation: Separates security perimeters into small zones governed by separate access rules. This network topology helps keep data secure by reducing the size of a system's attack

surface, breaking the network into multiple small pieces with each zone requiring separate access rules.

Monitoring and validation: Safe-T's SDP works to monitor, control, and audit user activities in real-time. If suspicious activities occur, the organization is alerted and can deny further access.

Example of Zero Trust Concepts



ZoneZero Perimeter Access Orchestration Solution

Safe-T's comprehensive Operational and Security suite; Perimeter Access Orchestration (PAO), is built and designed for implementing Zero-Trust Network Access (ZTNA).

Safe-T solutions in the PAO suite include:

ZoneZero SDP: Creates secure and transparent access workflows for any internal application, service, and data. Users must be successfully authenticated for a specific application before gaining visibility or access to that specific back-end service.

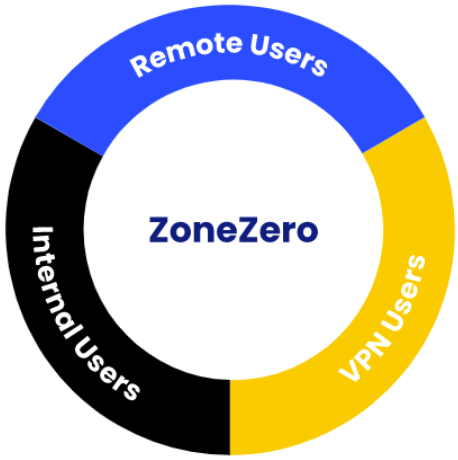
ZoneZero MFA: Integrates multifactor authentication and identity awareness into all access scenarios including for web and legacy non-web.

ZoneZero VPN: Enhances existing enterprise VPN systems via its application-layer policy monitoring and enforcement.

ZoneZero Reverse Access: Handles incoming requests without opening an incoming port on internal LAN firewall. The Access Controller pulls valid requests into the LAN over an outbound connection.

Safe-T Ltd. Patents: Implements micro-segmentation using a patented reverse access technology: Pat. https://www.Safe-T.com/the-Safe-T/.

Safe-T PAO Suite & Components:



SDP Features

Safe-T's SDP operates seamlessly with on-premises, in public or private cloud applications and resources.

Features include:

- Clientless – seamless implementation
- Supports multiple identity tiers in parallel
- Simple, cost effective, and secure deployment
- Based on Safe-T's patented Reverse Access
- Non-web protocols ready – SMB, RDP, SSH, REST API, any TCP
- Hybrid implementation
- Supports humans, applications, and connected devices
- Supports a variety of MFA capabilities: (SAML 2.0, OAuth 2.0, REST API)

Benefits

- Reduced operational costs
- Reduced attack surface
- Transparent solution
- Easily connects different types of users
- Improves data security by closing incoming firewall ports
- Scales precisely according to usage
- Fast deployment

- Enhances Zero Trust Network security

SDP Network Architecture is Growing in Popularity

Network architects, CISOs, and CTOs are weighing the advantages and costs of SDP solutions versus VPNs. Many want to implement an SDP solution but are reluctant to make the transition. This is because completely replacing a corporate VPN with an SDP can be both costly and disruptive to existing IT environments.

A recent survey performed by the Cloud Security Alliance (CSA) on the State of Software Defined Perimeter stated that the main obstacle for an organization wishing to implement SDP is the existence of pre-installed security technologies.

Another reason for transitioning to SDP is that there are new legislative regulations in certain jurisdictions that require companies to adopt a zero-trust architecture *by law*. For example, the following is a directive issued by a US government executive order:

Executive order

On May 12, 2021, an Executive Order 14028 was issued by US President Biden: "Improving the Nation's Cybersecurity". For government related organizations, implementing a Zero Trust architecture is now required by law.

If an organization operates or uses a US Federal Information System in a US federal agency, or as a government contractor, the Executive Order requires all organizations to develop a plan to migrate to a Zero Trust architecture.

Safe-T SDP And VPN Solutions Integration Approaches

The following sections describe two deployment options:

1. Integrating Zero Trust Capabilities Inline with an Existing VPN
2. Integrating Zero Trust and an Existing VPN, Side by Side for Different Categories of Users

Inline: Integrating Zero Trust capabilities inline with an existing VPN

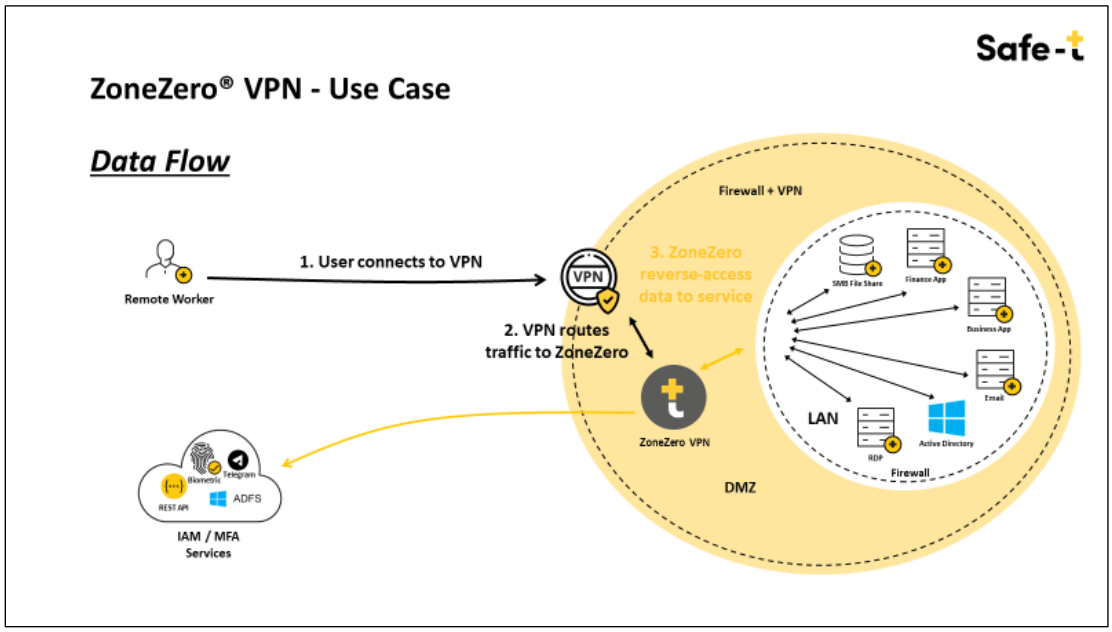
Safe-T's ZoneZero VPN solution provides a middle ground between keeping your company's VPN system or completely replacing it with a zero-trust solution.

This inline integration deployment option uses the Safe-T SDP solution to enhance your VPN security by adding SDP capabilities to yield a more fortified secure access infrastructure.

Safe-T's SDP is the only zero trust access solution in the market targeted at enhancing VPN security by adding zero trust capabilities.

Safe-T's SDP is deployed in the Demilitarized Zone (DMZ), isolated from other network segments. It is located after an organization's VPN gateway and before its internal firewall. Safe-T's SDP acts as a 'listener' to the VPN gateway and is transparent to the end user experience.

Example of Safe-T SDP and VPN inline architecture:



Side by side: Integrating Zero Trust and an existing VPN side by side for different categories of users

Hackers consider a company's third-party contactors, partners, and vendors relatively easy targets to breach. Third parties can be large security risks as they might not be aware of the organization's security rules and/or might not pay close attention to them.

Third parties usually do not require full access to a network. They usually require access only to specific back-end applications needed to perform their jobs.

This deployment option uses Safe-T SDP and the organization's VPN side by side. Long-term users such as employees can use an existing VPN system.

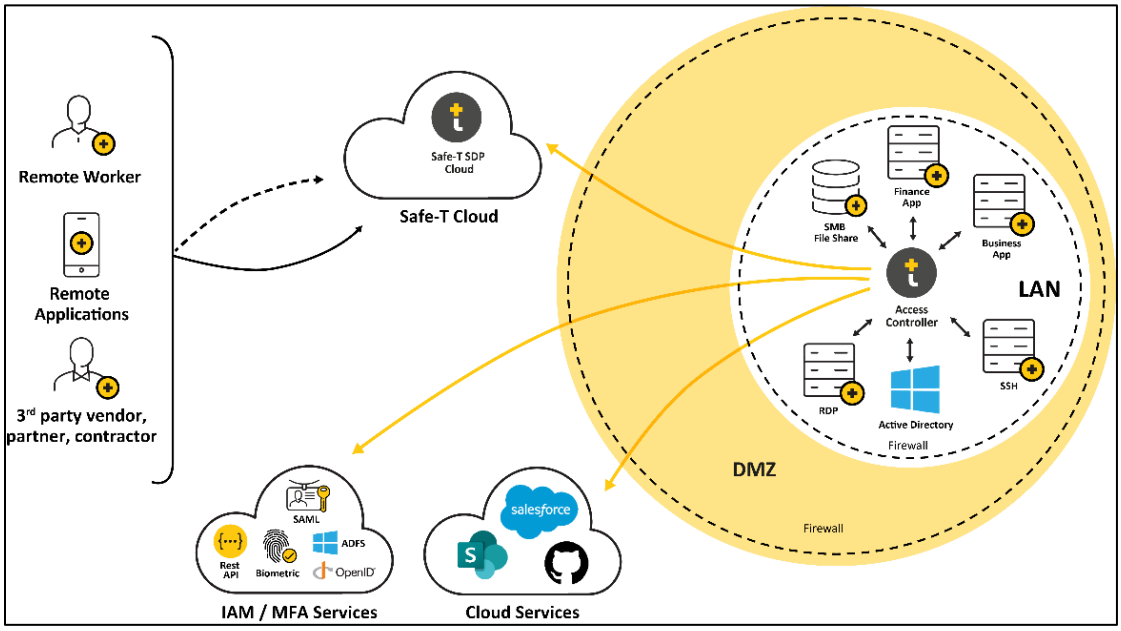
For these users, there is no need to change the IT infrastructure, and their user experience remains the same.

Using this deployment option, third parties are granted limited access to the organization's network. They login using Safe-T's SDP solution, not the company's VPN access. These users are granted narrow, granular, application access as determined by a Safe-T's SDP access control policy corresponding to the third-party's defined role.

As a result, the organization's VPN attack surface is significantly reduced, since third parties are not provisioned with a VPN client. A breach of the company's VPN gateway will not affect the

third-party users. This deployment option also enables organizations to test Safe-T's SDP solution in their environment. As a result, Safe-T solution's capabilities can be evaluated on a relatively small scale.

Example of the Safe-T SDP and VPN side-by-side architecture:



*The diagram shows third-party users, such as contractors and vendors, accessing only authorized applications using the Safe-T SDP solution.

Safe-T's Cyber Defense Awards

Safe-T Won 1st place in 2021 in two cyber defense categories:

- Access Control Hot Company
- Micro-segmentation Best Product

Reverse Access Patents

Safe-T's patented technology implements micro-segmentation using a unique, innovative reverse access technology. Users access back-end applications without opening inbound firewall ports. Pat. https://www.safe-t.com/the-Safe-T/

Conclusion

IT research analysts such as Gartner initially recommended a rip and replace model for a transition to an SDP architecture. However, Safe-T Ltd has taken the view that VPN replacement should not be the default deployment option. This is because SDP functionality can overlap with VPN capabilities.

Existing VPN solutions are not considered optimal because VPNs are vulnerable to hackers. However, Safe-T strongly believes there should be available middle ground options for network architects to choose from.

Safe-T's solutions provide a middle ground on a path towards SDP. The deployment options described in this white paper lower the risks and the cost of eventual SDP adoption starting with minimal infrastructure changes. This way, organizations can achieve the best of both SDP and VPN worlds.