Trout

Secure Remote Access: Essential VPN Guide for Industrial Cybersecurity

Introduction

The adoption of remote access technologies has transformed how industries manage and monitor critical infrastructure. From energy grids to manufacturing plants, remote work has become a necessity. In industrial environments, where physical presence was once essential, secure remote access offers significant benefits, including increased operational efficiency and reduced downtime. However, as reliance on remote work grows, so does the need to ensure these connections are properly secured to avoid cyber threats.

The Rise of Remote Access in Industrial Sectors

Between 2019 and 2021, the number of remote workers in the United States more than tripled, rising from approximately 9 million to 27.6 million people. This growth extends into industrial sectors such as energy, manufacturing, and utilities. For industrial operations, remote access is crucial. In the energy sector, for example, technicians responsible for monitoring multiple electricity generation sites rely on remote technologies to perform real-time maintenance and respond to incidents. Without remote access, organizations are physically limited and slowed down. This shift has allowed industries to remain efficient but has also increased the attack surface for cyber threats.

In manufacturing, remote access is equally valuable. For instance, a manufacturing company's sales team may need to access on-site production data to confirm inventory levels and provide real-time updates to customers. By remotely accessing this information, the sales team can efficiently process orders and address customer inquiries without needing to be physically present at the facility. This improves response times and enhances customer service but also requires secure access controls to protect sensitive operational data.

This rise in remote access across sectors highlights the dual challenge of efficiency and cybersecurity, underscoring the need for robust solutions that can securely manage remote connectivity in industrial environments.

The Need for Securing Remote Access in Industrial Environments

While remote access has improved operational efficiency, it introduces significant cybersecurity risks. Many industrial and manufacturing networks remain largely flat, relying on VLANs that offer only minimal segmentation and limited visibility into network activity. This lack of depth in network segmentation makes it easier for potential threats to move laterally once inside the network, exposing critical systems to higher risk. Additionally, vendors frequently maintain VPN connections to their devices for maintenance and monitoring purposes, further complicating security. These VPN bridges, though convenient, can become vulnerable entry points if not properly managed, making it crucial for industrial environments to adopt more robust segmentation and secure remote access practices.

One of the greatest challenges for IT and cybersecurity teams in industrial settings is balancing convenience with security requirements, and VPN implementation and management are a great example of that balance.

What is a VPN and How Does It Work?

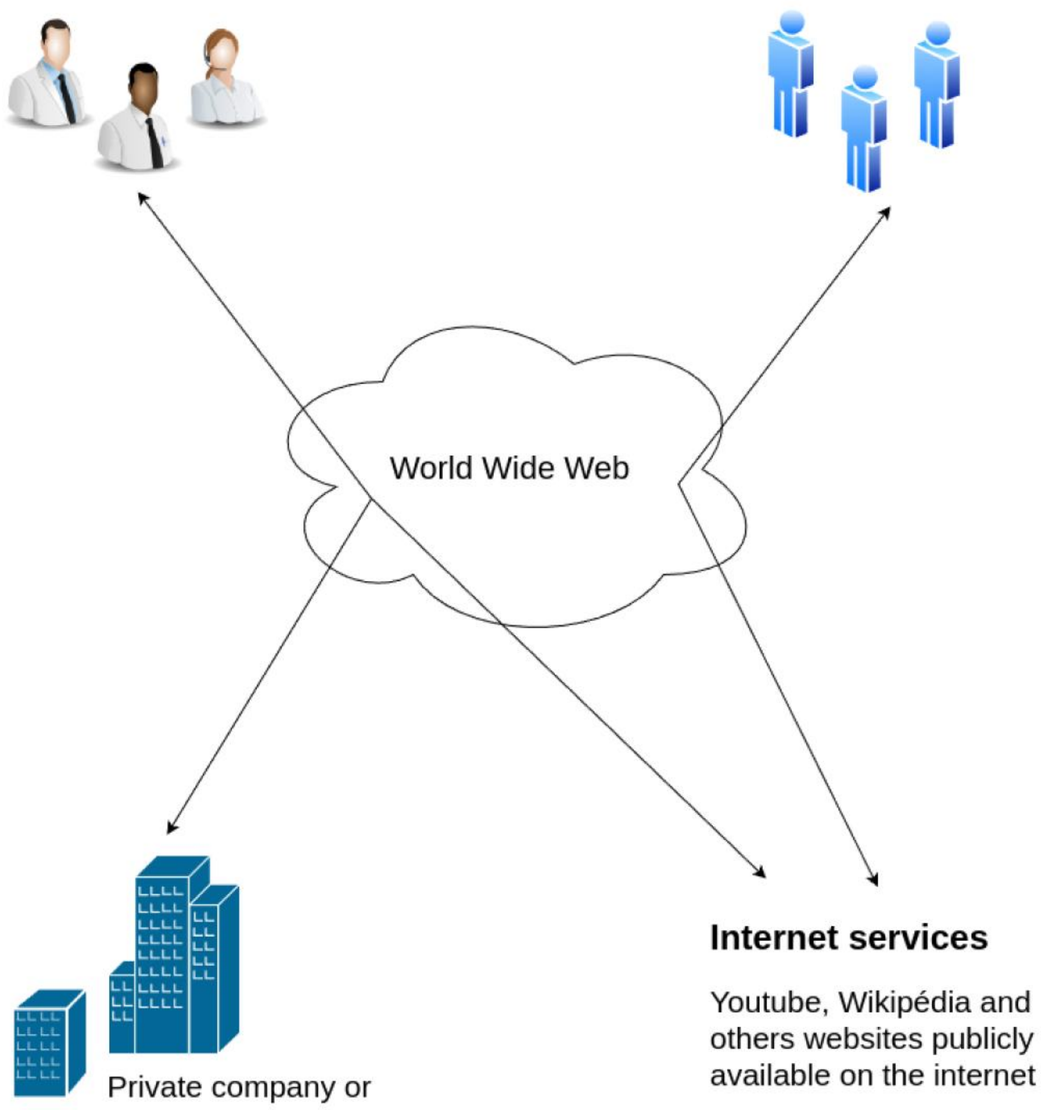


Figure 1: Simplified Workflow of Remote Access VPN in an Industrial Network

A Virtual Private Network (VPN) is a technology that provides secure, encrypted connections between a remote user and a corporate or industrial network. VPNs create a protected tunnel that shields data transmitted over public or less secure networks, ensuring that sensitive information cannot be intercepted by unauthorized parties. This is critical for industrial environments where operational technology (OT) systems need to remain accessible yet secure from cyber threats.

A typical VPN setup includes a VPN client on the user's device and a VPN gateway at the network's edge. When a user initiates a connection, the VPN client encrypts the data before sending it through the public internet to the VPN gateway, which decrypts it and forwards it to the internal network. This encrypted tunnel ensures that even if data is intercepted, it cannot be read or altered by unauthorized individuals.

The Need for Securing Remote Access in Industrial Environments

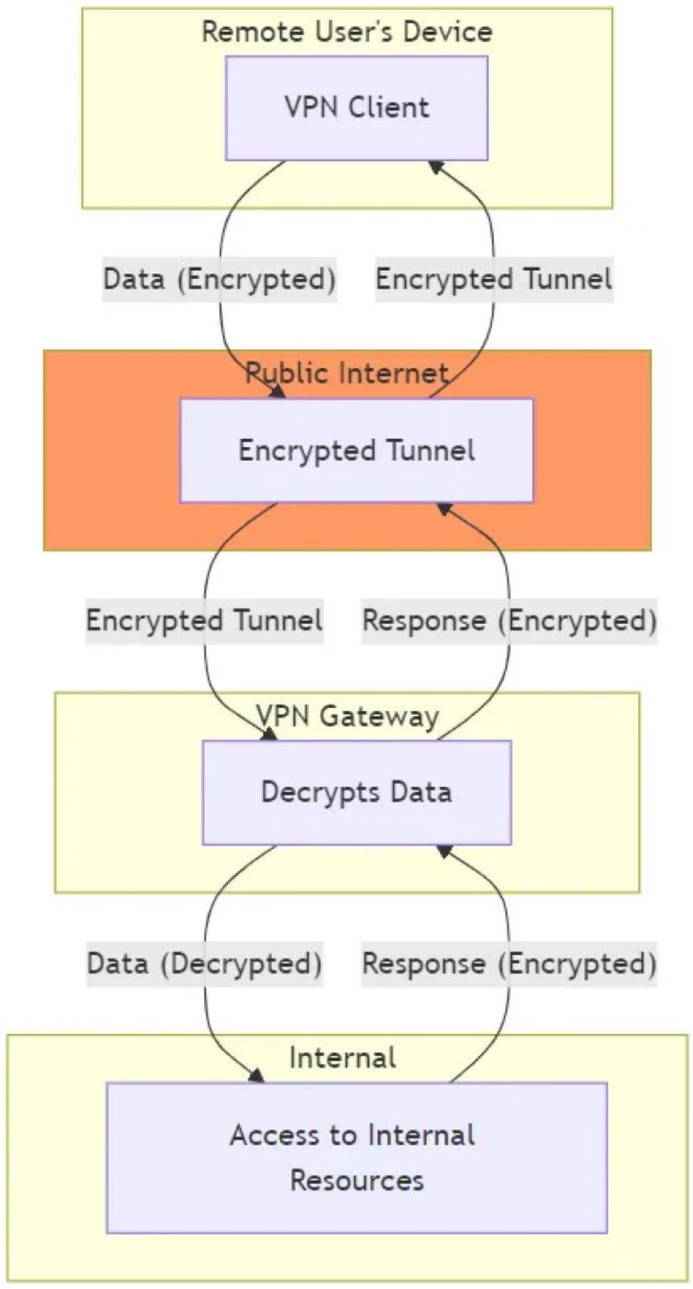


Figure 2: Data Flow Through a Remote Access VPN for Secure Access to Internal Resources

Risks

Component	Risk
Remote User's Device (VPN Client)	Device Compromise, Weak VPN Client Configuration
Public Internet (Encrypted Tunnel)	Weak Encryption Protocols or Algorithms
Public Internet (Encrypted Tunnel)	Man-in-the-Middle Attacks or Traffic Analysis
VPN Gateway (Decrypts Data)	VPN Gateway Compromise, Improper Configuration
Internal Access to Internal Resources	Internal Network Threats, Lateral Movement
Internal Access to Internal Resources	Sensitive Data Exposure at Rest

Table 1: VPN Components and Associated Security Risks in Figure 2

Note on VPN Confidentiality:

While VPNs are commonly associated with personal privacy and bypassing geographic restrictions in the collective mind, their primary purpose is to ensure confidentiality by encrypting data. This encryption prevents unauthorized access, even over public networks, which is valuable for safeguarding sensitive information in both personal and industrial contexts.

VPN Vulnerabilities and Security Risks

Common Vulnerabilities in VPNs

Despite their importance, VPNs can become significant security liabilities due to factors such as outdated encryption, misconfigurations, and weak credentials. These vulnerabilities can stem from poor implementation or lack of ongoing maintenance, but also stem from the actual nature of a VPN, which creates a network bridge and flattens a network to a remote endpoint.

1. Outdated Encryption: VPNs rely on encryption to secure data in transit. However, outdated encryption protocols, such as older versions of IPsec or SSL, can be exploited by attackers to intercept and manipulate data. It is essential to use the latest encryption methods to protect sensitive data.

2. Misconfigurations: Poorly configured VPNs can expose vulnerabilities within the network, making unauthorized access easier. Common misconfigurations include improperly set access controls or firewall settings that leave critical OT systems exposed.

3. Weak Credentials: One of the most common entry points for attackers is through compromised or weak credentials. Passwords that are easily guessed or not protected by multi-factor authentication (MFA) make it easier for attackers to escalate privileges and access sensitive OT systems.

VPNs, while useful for secure remote access, inherently flatten a network by creating broad, unrestricted tunnels that allow direct communication across various network segments. This design contradicts the principles of micro-segmentation, which aims to isolate network segments and control communication between them to minimize security risks.

Emerging Security Approaches: SDP and AI-Powered Monitoring

In addition to VPNs, Software-Defined Perimeter (SDP) solutions and AI-powered monitoring systems are emerging as stronger alternatives for securing remote access.

- SDP (Software-Defined Perimeter): SDP solutions operate on a zero-trust principle, where access is granted based on strict identity verification and not network location. This method isolates resources from unauthorized users, making lateral movement across the network more difficult. SDP dynamically creates secure connections based on user authentication, minimizing the risks of VPN misconfigurations and credential-based attacks.

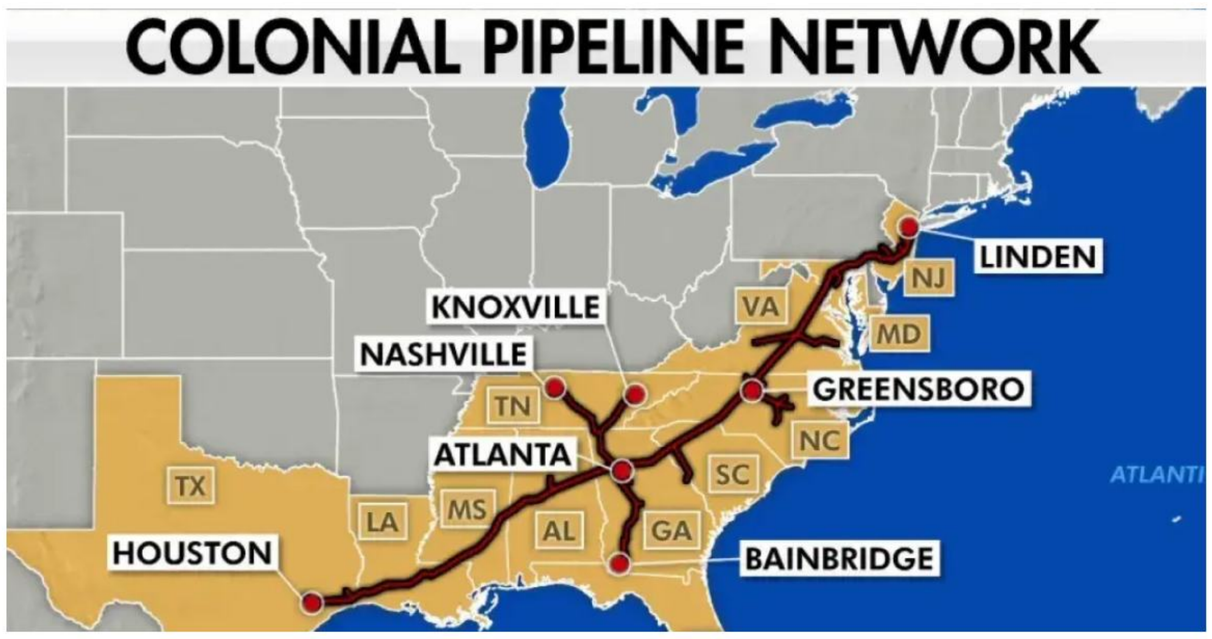
- AI-Powered Monitoring: AI and machine learning are being increasingly used to enhance monitoring systems. AI can detect anomalies in real-time and predict potential vulnerabilities before they are exploited, significantly improving the responsiveness of cybersecurity teams. AI-powered monitoring of VPN traffic ensures early detection of attacks, reducing the potential damage.

- VPN to DMZ with Proxy: Limiting VPN access to a DMZ establishes a secure buffer zone that restricts external access to specific, isolated resources while keeping internal networks shielded. If access to internal systems is required, a proxy server within the DMZ can act as an intermediary, allowing controlled, monitored connections without exposing the core network. This layered approach reduces the risk of unauthorized lateral movement by isolating sensitive assets behind the DMZ and routing traffic through the proxy.

Notable Incidents: Colonial Pipeline Attack and CDK Global Breach

The real-world consequences of VPN vulnerabilities are demonstrated by high-profile incidents, such as the Colonial Pipeline attack and the CDK Global breach, which show how devastating VPN exploitation can be.

Colonial Pipeline Attack (2021):



The Colonial Pipeline attack remains one of the most significant cybersecurity breaches targeting U.S. critical infrastructure. On May 7, 2021, the pipeline, which supplies nearly half of the East Coast's fuel, was crippled by a ransomware attack, forcing operations to shut down for several days. This disruption led to widespread fuel shortages, affecting millions of consumers and businesses and prompting the declaration of a state of emergency by President Joe Biden.

The attackers exploited a compromised password for an unused VPN account that was not protected by multi-factor authentication (MFA). This weak point in Colonial Pipeline's security architecture allowed the attackers, later identified as part of the DarkSide group, to gain remote access to the network. Once inside, they moved laterally across the IT environment, encrypting key systems and demanding a ransom. Key vulnerabilities that contributed to the attack include:

- Lack of MFA: The VPN account did not have multi-factor authentication enabled, making it easier for attackers to gain access using stolen credentials.
- Poor Password Management: The VPN account had not been decommissioned, despite being inactive, leaving a door open for attackers.
- Insecure Remote Access Practices: Remote access tools and configurations, especially in hybrid IT-OT environments, are often not designed with security-first principles, creating potential entry points for attackers.

This incident highlights the dangers of inadequate remote access security, especially in operational technology (OT) environments where downtime can lead to far-reaching consequences. It demonstrates the need for comprehensive cybersecurity measures, including MFA, network segmentation, regular patching, and continuous monitoring of remote access systems to detect unusual activity early.

CDK Global Breach (2024):

In June 2024, CDK Global, a leading SaaS provider for the automotive industry, suffered two consecutive ransomware attacks. The cybercriminal group BlackSuit was identified as the perpetrators, demanding a ransom in the tens of millions. The attacks impacted thousands of car dealerships across North America, paralyzing critical operations such as financing, payroll, and inventory management, all of which rely on CDK's cloud-based software platform.

One of the core vulnerabilities exploited in these attacks was CDK's always-on VPN connections, which dealerships use to maintain continuous access to CDK's data centers. This always-on configuration, while designed for operational efficiency, also created a persistent security risk:

- Always-On VPN Exposure: These VPNs, designed to maintain uninterrupted access between dealership systems and CDK's data centers, left a wide attack surface. The persistent connection provided attackers with continuous access to the network once compromised.
- Auto-Update Privileges: CDK's software had automatic update capabilities, requiring elevated privileges similar to admin rights. Once attackers gained access, this auto-update feature likely accelerated their ability to spread ransomware and affect multiple systems at scale.
- Lack of Network Segmentation: With continuous VPN connections and administrative privileges, attackers were able to move freely between dealerships and CDK's central systems, causing widespread disruption.

In response, CDK instructed dealerships to disconnect from their data centers as a precautionary measure during the incident. However, the attack demonstrates the critical risks of always-on VPN infrastructures, especially when not paired with multi-factor authentication (MFA), network segmentation, and continuous monitoring.

This attack underscores the necessity of securing remote connections, particularly in SaaS environments where clients depend on continuous access. Implementing zero-trust architectures, restricting elevated privileges, and regularly reviewing remote access policies could help mitigate the risks of such large-scale attacks in the future.

Known CVEs Impacting VPNs

Several Common Vulnerabilities and Exposures (CVEs) have been identified that exploit weaknesses in VPN implementations. These CVEs highlight the importance of regular patching and vigilant security practices.

- CVE-2024-24919 (Check-Point VPN): This zero-day vulnerability allowed attackers to exploit Check Point VPN gateways, exposing critical information about network security configurations. Exploited since April 2024, this vulnerability allowed hackers to enumerate and extract password hashes, significantly increasing the risk of credential theft and unauthorized access.
- CVE-2023-46805 and CVE-2024-21887 (Ivanti VPN): These zero-day flaws in Ivanti Connect Secure VPN devices enabled unauthenticated remote code execution, allowing attackers to bypass security measures and take full control of the affected devices. Exploited to deliver malware, these vulnerabilities highlighted the importance of timely patching and updating VPN appliances.
- CVE-2024-3661 (TunnelVision): This vulnerability revealed that certain VPNs could be bypassed, exposing user traffic to potential interception. TunnelVision exploited weaknesses in VPN encapsulation by rerouting traffic outside the encrypted tunnel, leaving sensitive data unprotected. The vulnerability had existed undetected for over 20 years, showing that even long-trusted VPN technologies can harbor deep-seated flaws.
- CVE-2022-42475 (FortiOS SSL/VPN): A recent zero-day vulnerability in a popular VPN system enabled remote code execution through a heap-based buffer overflow. Affecting multiple ICS software versions, the flaw was exploited against organizations, including government entities, allowing attackers to breach systems via crafted requests. This incident underscores the critical need for securing VPNs in corporate and industrial networks and highlights the importance of regular patching and proactive monitoring.
  Check out this article that delves deeper into the Flaw.

💡The Akira Ransomware Threat

A recent example underscores the importance of securing VPN infrastructure: Akira ransomware has exploited known vulnerabilities in VPN appliances, to gain initial access. In some cases, systems without multi-factor authentication (MFA) are especially at risk.

Trout

Mitre ATT&CK Mapping & Cyber Kill Chain

Tactic	Technique	Technique Name	Context
TA0108 / TA0109	T0866	Exploitation of Remote Services	An exploited VPN constitutes an exploitation of remote services.
TA0108	T0822	External Remote Services	A compromised VPN typically involves exploiting vulnerabilities in a service exposed to the external network, as VPNs serve as gateways for external access to internal resources.
TA0111	T0890	Exploitation for Privilege Escalation	Attackers often use VPN exploitation to escalate privileges.
TA0109 / TA0110	T0859	Valid Accounts	Attackers may use valid, compromised credentials to access private networks. For example, the Colonial Pipeline attack involved the exploitation of VPNs using compromised credentials.
TA0102	T0846	Remote System Discovery	Once inside the network, attackers usually conduct reconnaissance of the system and network to discover additional targets.
TA0109	T0867	Lateral Tool Transfer	If attackers use tools to move laterally within the network, this technique applies.
TA0102	T0840	Network Connection Enumeration	Vulnerabilities, such as the Check Point VPN Vulnerability, allow attackers to enumerate and extract information from VPN gateways.
TA0104	T0842	Command-Line Interface	Adversaries may use command-line interfaces (CLIs) to interact with systems and execute commands.
TA0102	T0842	Network Sniffing	Attackers may exploit flaws to sniff network traffic that should have been encrypted by the VPN.
TA0107	T0807	Device Restart/Shutdown	Attackers may exploit flaws to sniff network traffic that should have been encrypted by the VPN.
TA0107	T0838	Service Stop	Attackers may exploit flaws to sniff network traffic that should have been encrypted by the VPN.
TA0107	T0881	Modify Alarm Settings	Attackers may exploit flaws to sniff network traffic that should have been encrypted by the VPN.
TA0107	T0814	Denial of Service	Attackers may target VPN infrastructure with denial-of-service (DoS) attacks, overwhelming it with traffic or using the compromised VPN to launch DDoS attacks against internal resources.
TA0103 / TA0106	T0856	Spoof Reporting Message	In control system environments, adversaries may spoof reporting messages to evade detection or impair process control.
TA0105	T0879	Damage to Property	Adversaries may cause damage or destruction to infrastructure, equipment, and surrounding environments during control system attacks.
TA0105	T0882	Theft of Operational Information	Once inside the VPN, adversaries may steal operational information related to production environments for personal gain or to inform future operations.

1. **Recon (Initial Access):**
   - TA0102 - T0840 Network Connection Enumeration: Attackers exploit VPN vulnerabilities to enumerate and extract information from VPN gateways. This falls under the Recon category in the Cyber Kill Chain.

2. **Weaponization:**
   - TTP: TA0108 - T0822 External Remote Services: When a VPN is compromised, it typically involves exploiting vulnerabilities in a service exposed to the external network. This falls under the Weaponization category in the Cyber Kill Chain.

3. **Delivery:**
   - (None of the listed techniques directly fit this category.)

4. **Exploitation:**
   - TTP: TA0108 - T0866 Exploitation of Remote Services: An exploited VPN is categorized as Exploitation of Remote Services. This falls under the Exploitation category in the Cyber Kill Chain.

   - TTP: TA0111 - T0890 Exploitation for Privilege Escalation: Attackers often use VPN exploitation to escalate privileges. This falls under the Exploitation category in the Cyber Kill Chain.

   - TTP: TA0109 - T0859 Valid Accounts: Attackers use compromised credentials to access private networks. This falls under the Exploitation category in the Cyber Kill Chain.

5. **Installation:**
   - (None of the listed techniques directly fit this category.)

6. **Post-Exploitation (Command and Control):**
   - TTP: TA0102 - T0846 Remote System Discovery: Once inside, attackers conduct reconnaissance of the system and network. This falls under the Post-Exploitation category in the Cyber Kill Chain.

   - TTP: TA0109 - T0867 Lateral Tool Transfer: If attackers use tools to move laterally within the network, this technique applies. This falls under the Post-Exploitation category in the Cyber Kill Chain.

   - TTP: TA0102 - T0842 Network Sniffing: Attackers may exploit the vulnerability to sniff network traffic that should have been encrypted by the VPN. This falls under the Post-Exploitation category in the Cyber Kill Chain.

   - TTP: TA0104 - T0807 Command-Line Interface: Adversaries may use command-line interfaces (CLIs) to interact with systems and execute commands. This falls under the Post-Exploitation category in the Cyber Kill Chain.

7. **Actions on Objectives:**

- TTP: TA0107 - T0816 Device Restart/Shutdown: Adversaries may forcibly restart or shut down a device in an ICS environment, disrupting and negatively impacting physical processes. This falls under the Actions on Objectives category in the Cyber Kill Chain.

- TTP: TA0107 - T0838 Modify Alarm Settings: Adversaries may modify alarm settings to prevent alerts that would notify operators of their presence or prevent responses to dangerous scenarios. This falls under the Actions on Objectives category in the Cyber Kill Chain.

- TTP: TA0107 - T0881 Service Stop: Adversaries may stop or disable services on a system, rendering them unavailable to legitimate users. This falls under the Actions on Objectives category in the Cyber Kill Chain.

- TTP: TA0107 - T0814 Denial of Service: Attackers can target VPN infrastructure, overwhelming it with traffic to disrupt operations and deny legitimate access. Alternatively, the compromised VPN can be used as a vector for launching DDoS attacks on internal resources or other systems within the network. This falls under the Actions on Objectives category in the Cyber Kill Chain.

- TTP: TA0105 - T0879 Damage to Property: Adversaries may cause damage or destruction to infrastructure, equipment, and the surrounding environment when attacking control systems. This falls under the Actions on Objectives category in the Cyber Kill Chain.

- TTP: TA0105 - T0882 Theft of Operational Information: Once inside the VPN, adversaries may steal operational information from production environments for personal gain or to inform future operations. This falls under the Actions on Objectives category in the Cyber Kill Chain.

- TTP: TA0103 - T0856 Spoof Reporting Message: Adversaries may spoof reporting messages in control system environments to evade detection or impair process control. This falls under the Actions on Objectives category in the Cyber Kill Chain.

Mitigations for Securing VPNs in Industrial Environments

Mitigating security risks associated with VPNs requires a multi-layered approach that incorporates best practices in network architecture, authentication, monitoring, and regular maintenance. The following strategies are essential for reducing the attack surface and enhancing security for VPN deployments in industrial environments.

Zero-Trust Network Access

Implementing a zero-trust architecture is fundamental in preventing unauthorized access to critical systems. In a zero-trust model, no user or device, whether inside or outside the network, is automatically trusted. Instead, every access request must be authenticated, authorized, and continuously monitored.

-Granular Access Enforcement:
Users are given access only to specific systems they need to perform their tasks, reducing the potential for unauthorized accesses. This ensures that even if a VPN account is compromised, the attacker cannot freely explore the entire system.

-Role-Based Access Control (RBAC):
Implement RBAC policies that assign access based on the specific roles within the organization. For example, technicians may have access only to machines they need for their tasks, while administrative access to other systems is restricted.

Network Segmentation and Demilitarized Zones (DMZ)

Network segmentation is vital in limiting the potential damage if an attacker gains access through a VPN. By isolating critical systems from general network traffic, the exposure of sensitive IT and OT systems is minimized.

- Network Isolation: Separate IT and OT networks by granular use cases using firewalls, access controls, or Trout's CyberSwitch solution (😉), creating distinct security zones. Core infrastructure, such as production systems, should not be accessible from external networks without strong controls and a proxy architecture in place.
- DMZ in front of each subnetwork: Implement a Demilitarized Zone (DMZ) to host services that are exposed to external users, while isolating the most sensitive systems. This approach helps prevent attackers from moving laterally across networks after initial infiltration.

Multi-Factor Authentication (MFA) for VPN Access

Multi -factor authentication (MFA) is one of the most effective security measures to prevent unauthorized VPN access. By requiring users to authenticate through two or more verification methods, the risk of compromised credentials is minimized.

- MFA Reduces Credential-Based Attacks: In sensitive environments like manufacturing sites, MFA ensures that even if a VPN password is stolen or guessed, unauthorized users cannot gain access without the additional authentication factor. This would have mitigated the Colonial Pipeline attack, where a compromised password without MFA allowed attackers to access critical systems.

Monitoring and Detection Systems

Continuous monitoring of VPN traffic and system access is critical for early detection of anomalous behavior that could indicate a cyberattack. Deploying Intrusion Detection and Prevention Systems (IDS/IPS) helps organizations detect and respond to threats.

- Intrusion Detection and Prevention: IDS/IPS solutions monitor VPN traffic for signs of malicious activity, such as repeated login failures or unauthorized access attempts. In the event of unusual activity, these systems can trigger alerts or block malicious traffic.

- Logging and Activity Analysis: Maintain detailed logs of VPN connections, including login attempts, and evaluate the ability to correlate to other systems to identify accessed resources. This data helps trace unauthorized access and supports incident response efforts. Comprehensive logging also enables forensic investigations if a breach occurs.

Regular Patch and Update Management

Maintaining up-to-date software and security patches is critical for mitigating vulnerabilities in VPN systems. Many attacks, such as the Ivanti VPN vulnerability (CVE-2023-46805) and Check-Point VPN vulnerability (CVE-2024-24919), have exploited known but unpatched vulnerabilities.

- Patch Management Schedule: Establish a patch management schedule to ensure VPN software and associated systems are updated. Regular updates reduce the likelihood of attacks exploiting outdated software.

Principle of Least Privilege (PoLP)

Applying the principle of least privilege (PoLP) ensures that users and systems only have the minimum access necessary to perform their tasks. This minimizes the risk of excessive access permissions being abused by attackers.

- Access Control Policies: Define and enforce access control policies that limit VPN users to only the resources necessary for their roles. For example, a field technician might have access to specific machine but would be restricted from other resources.

Measurable Benefits of VPNs for Industrial Remote Access

VPNs are essential for securing remote access in industrial environments, providing both operational and security benefits. Here are some quantifiable improvements companies have experienced by implementing VPN solutions:

- Operational Uptime: Up to 50% Reduction in Downtime

Research by the Aberdeen Group shows that manufacturers using remote monitoring and diagnostics through secure access solutions, like VPNs, reduced unplanned downtime by 50%, resulting in significant productivity gains. This decrease in downtime allows for quicker identification and resolution of issues, enhancing operational continuity.

- Cost Savings: 25-30% Reduction in Travel and Site Visit Costs

According to Gartner, organizations that implement remote access solutions can reduce their site visit and travel costs by 25-30%, as fewer onsite technician visits are needed for monitoring or troubleshooting. This reduction in travel not only cuts expenses but also lowers environmental impact through reduced fuel consumption.

- Improved Response Times

VPNs allow immediate access to operational systems, enabling technicians to respond to issues in real-time. According to a study by Honeywell Process Solutions, remote access technologies have improved response times by 30-40% in critical situations, minimizing downtime and mitigating risks to operational continuity.

How to Set Up and Deploy a VPN for Industrial Remote Access

Setting up a Virtual Private Network (VPN) in industrial environments requires a comprehensive approach that addresses both security and operational needs. The deployment process must ensure that the VPN solution is robust, scalable, and capable of supporting the unique demands of industrial networks, such as operational technology (OT) systems and geographically dispersed sites. In this section, we will provide a step-by-step guide for deploying a VPN and outline how to scale the solution across multiple locations.

Step-by-Step Guide for VPN Deployment

To deploy a VPN for industrial remote access, it is essential to follow a structured process that ensures secure configuration and monitoring of the VPN infrastructure. Here's a breakdown of the key steps:

1. **Evaluate Requirements and Choose the Right VPN Solution**
   - Determine Connectivity Needs: Assess the number of remote users, locations, and type of access they require (e.g., full network access or specific segments). This will help guide decisions on VPN architecture and scalability.

2. **Install and Configure the VPN Software**
   - Deploy VPN Server: Install the VPN server on a dedicated machine within the network. Ensure the server has sufficient resources to handle encryption and traffic flow, and install the necessary VPN software (e.g., OpenVPN, Cisco AnyConnect).
   - Configure Secure Access Controls: Set up the VPN to support secure protocols (e.g., IPsec or SSL) to ensure encrypted data transmission.

3. **Configure Secure Access Controls**
   - User Authentication: Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to verify user identities before granting VPN access. This reduces the risk of unauthorized access, especially for users connecting to sensitive systems remotely.
   - Access Control Policies: Define granular access control policies to limit VPN users to only the resources they need. For instance, technicians might be restricted to accessing specific machinery. Use role-based access control (RBAC) to enforce these policies.
   - Encryption: Ensure VPN connections use robust encryption protocols, such as WireGuard or IPsec, to secure data in transit. Configure the VPN to automatically reject weak encryption methods that could compromise data security.

4. **Monitor and Log VPN Activity**
   - Continuous Monitoring: Deploy monitoring tools to track VPN activity and detect anomalies that may indicate potential security breaches. Real-time alerts can help catch suspicious behavior, like repeated failed login attempts or unusual traffic patterns.
   - Logging and Audit Trails: Maintain detailed logs of VPN sessions, including users accessing the network, session durations, and resources accessed. This information is critical for compliance and incident response.

Ensuring Scalability Across Multiple Sites

In industrial settings, VPNs are often deployed to support multiple remote sites, which may be geographically dispersed. Ensuring that the VPN infrastructure can scale to meet these demands is crucial for maintaining secure and efficient operations.

1. **Tailoring VPN Configurations for Remote Sites**
   - Hub-and-Spoke Architecture: For environments with multiple remote locations, consider deploying a hub-and-spoke architecture, where each remote site (spoke) connects to a central VPN hub at headquarters. This allows for centralized management of the VPN while ensuring that remote sites have secure access to the necessary resources.Site-to-Site
   - VPNs: For highly dispersed sites that need direct communication with each other (e.g., interconnected factories or power plants), set up site-to-site VPNs to facilitate secure data exchanges between locations without routing traffic through a central hub. This reduces latency and improves network performance.

2. **Load Balancing and Redundancy**
   - Load Balancing: As the number of VPN users and sites increases, implement load balancing to distribute traffic across multiple VPN servers. This prevents any single server from becoming a bottleneck and ensures that the VPN infrastructure can handle the demands of multiple users simultaneously.
   - Redundancy and Failover: In critical industrial environments, downtime can have severe operational impacts. Implement redundant VPN servers and failover mechanisms to ensure that the network remains operational even if one VPN server goes down. This is especially important for industries where remote access is required for real-time monitoring and control of OT systems.

3. **VPN Bandwidth Optimization**
   - Traffic Prioritization: Industrial environments often require that certain types of traffic, such as control signals for OT systems, take priority over less critical data. Implement Quality of Service (QoS) to prioritize traffic within the VPN, ensuring that essential operations are not affected by congestion.
   - Optimizing Performance: Regularly assess the VPN infrastructure's performance to ensure that it can handle the required bandwidth. As more sites and users are added, upgrade VPN hardware or increase network bandwidth to prevent slowdowns.

Conclusion

Increasingly connected industrial environments require secure remote access to manage operational technology (OT) systems. VPNs are a foundational element in ensuring the security of these remote connections, but they should be seen as part of a broader, layered cybersecurity strategy.

VPNs as a Key Component of Cybersecurity

VPNs create secure, encrypted tunnels to protect data in transit, making them indispensable for industrial environments. However, they are not foolproof. A robust security posture combines VPNs with complementary measures such as multi-factor authentication (MFA), network segmentation, and zero-trust architecture:

- MFA strengthens user verification, minimizing the risk of unauthorized access.
- Network segmentation isolates critical OT systems, reducing the potential for lateral movement in case of a breach.
- Zero-trust models ensure that access is constantly verified, preventing assumptions of trust within or outside the network.

Ongoing Monitoring and Patching

Continuous monitoring of VPN traffic for unusual behavior is crucial for early threat detection. In addition, applying regular patches ensures that VPN vulnerabilities are addressed before they are exploited. This is especially important as new vulnerabilities such as CVE-2024-24919 continue to emerge.

Final Thoughts

VPNs remain vital for securing remote access in industrial settings. However, they must be continuously strengthened with layered security measures, ongoing updates, and advanced solutions like the Trout secure network overlay to stay resilient against evolving threats. By integrating these practices, organizations can protect critical infrastructure while maintaining operational efficiency.


Trout