IntegraONE

35 YEARS OF TECHNOLOGY EXCELLENCE

THANK YOU FOR BEING A PART OF OUR STORY 1990 • 2025

SECURING VPN ACCESS

ONE CON 2025

managing
complexity
delivering

simplicity

IntegraONE

Thank You for Joining!

Join us for a live demo on how to protect your remote workforce with secure VPN access. We'll showcase how we secure access for your remote workforce now and discuss how to approach it moving forward.

IntegraONE

INTRODUCTION

Andrew Dreibelbis

MSP Networking Team Lead

I joined IntegraOne in 2022 as a member of the MSP Network team and have taken over the role of Team Lead earlier this year. I provide guidance and assistance to my team of 6 engineers and collaborate with our PS team for projects and complex issues.

I hold certifications in multiple Fortinet products as well as an Azure Networking Engineering certificate. I have experience with multiple firewall vendors, switching, and wireless networking with Fortinet/Aruba/Meraki.

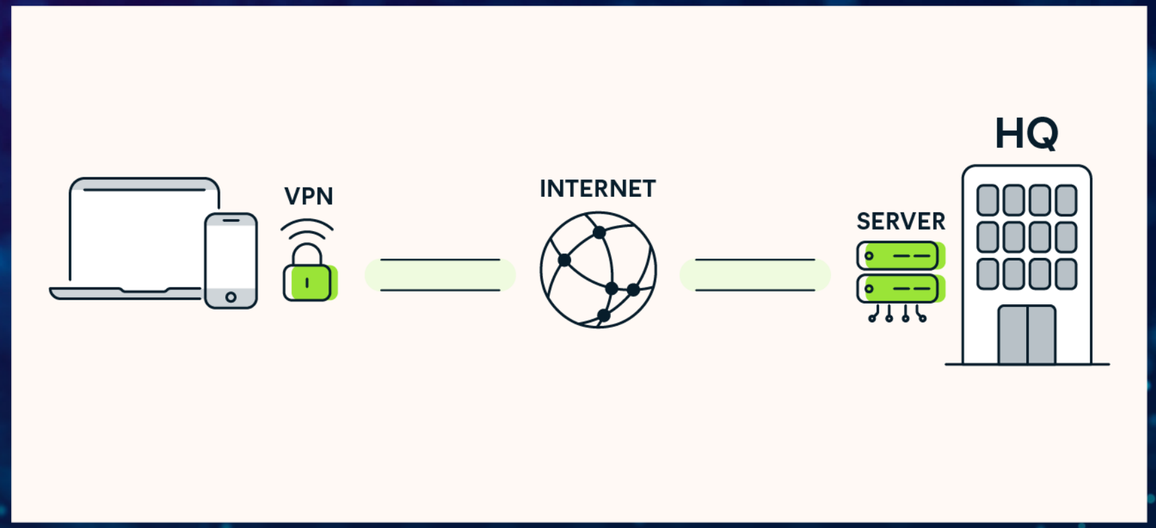
IntegraONE

Goals

- Why we need remote access?
- Why do we use SSLVPN?
  - Pros
  - Cons
- Mitigating SSLVPN issues – demo
  - Negative impact of bot traffic on firewall performance
  - Geo restrictions
  - Putting SSLVPN on Loopback
  - Blocking known threats with ISDB objects (and/or threat feeds)
  - Utilizing MFA
- What's next?
  - Dial-up Ipsec
  - ZTNA/SASE
  - EMS
- Conclusion and Q&A

IntegraONE

Why do we need Remote Access?



- Flexibility for remote workers, students, and anyone needing to connect to internal company systems or resources from outside the physical office
- You need a VPN to securely access private networks and sensitive data from a remote location by encrypting your internet connection and authenticating your identity.
- SSL VPNs create an encrypted tunnel, protecting your data from being intercepted by malicious actors when you're on public Wi-Fi or other unsecured networks

IntegraONE

Why do we use SSLVPN?

Feature	SSL VPN Benefit
Encryption	Uses HTTPS (TLS/ SSL)
Accessibility	Works anywhere via web browser
Firewall Friendly	Uses port 443 —rarely blocked
Clientless Option	No need to install VPN client
Ease of Setup	Easier than IPsec for remote access
Granular Permissions	Per-user/ group access control
Compatibility	Supports mobile and desktop devices

IntegraONE

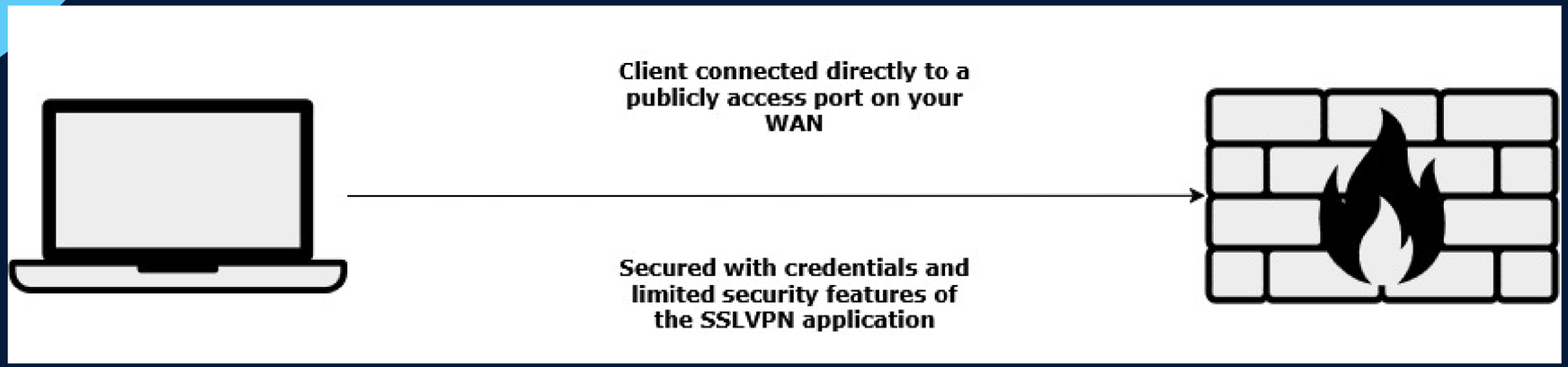
Why do we use SSLVPN?

Limitation	Explanation
Limited in Clientless Mode	Only web apps, no full network access
Requires Client for Full Access	Must install software for full tunneling
Slower Performance	SSL adds overhead, may be slower than IPsec
Critical vulnerabilities	Requires frequent patching
Session Stability	Prone to disconnects over poor connections
Exposed to the public Internet	Common target for cybercriminals

IntegraONE

Mitigating SSLVPN Risks

Understand how the traffic flows



IntegraONE

Mitigating SSLVPN Risks

Understand how the traffic flows

IntegraONE

Demo Info

- Created a virtual firewall in Azure to track results from different configurations
- Left the firewall exposed with basic SSLVPN configuration for 24 hours
- Introduced SSLVPN loopback and firewall rules to restrict traffic
- Transitioned to dial-up Ipsec
- https://badfirewall.dreib.net

IntegraONE

Demo Info

- Base configuration quickly became unusable
  - CPU spikes and high memory usage

General System Events

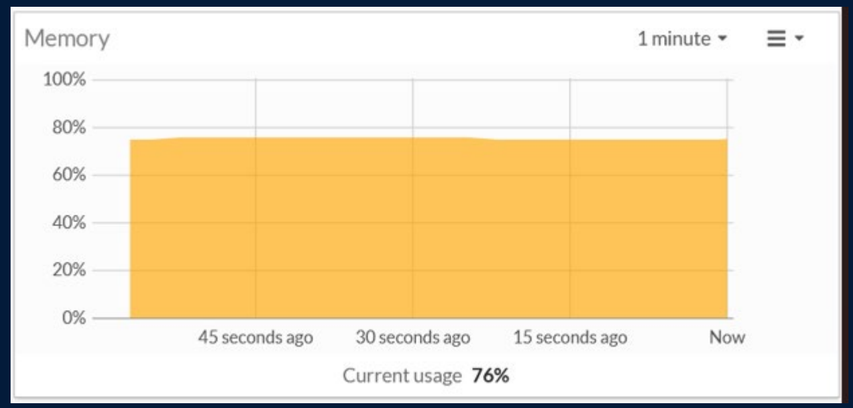
Top Event	Level	Count
Admin login failed	Alert	5,461
Admin login disabled	Alert	789
FortiGate update succeeded	Notice	70
DHCP statistics	Information	48
CPU usage statistics	Notice	12

6,400 events

VPN Events

Top Event	Level	Count
SSL VPN alert	Error	7,235
SSL VPN new connection	Information	2,337
SSL VPN exit error	Error	27

9,599 events



IntegraONE

Securing SSLVPN

- Move the SSLVPN interface to a loopback
  - Create firewall rules to block bad actors
  - Introduce Geographic restrictions
  - Enable security profiles
  - Disable web-based SSLVPN and disable the web portal
- Disable web-based SSLVPN and break the web portal
- Use Multi-factor authentication

Microsoft Authenticator

IntegraONE

What’s next?

- Dial-up IPsec

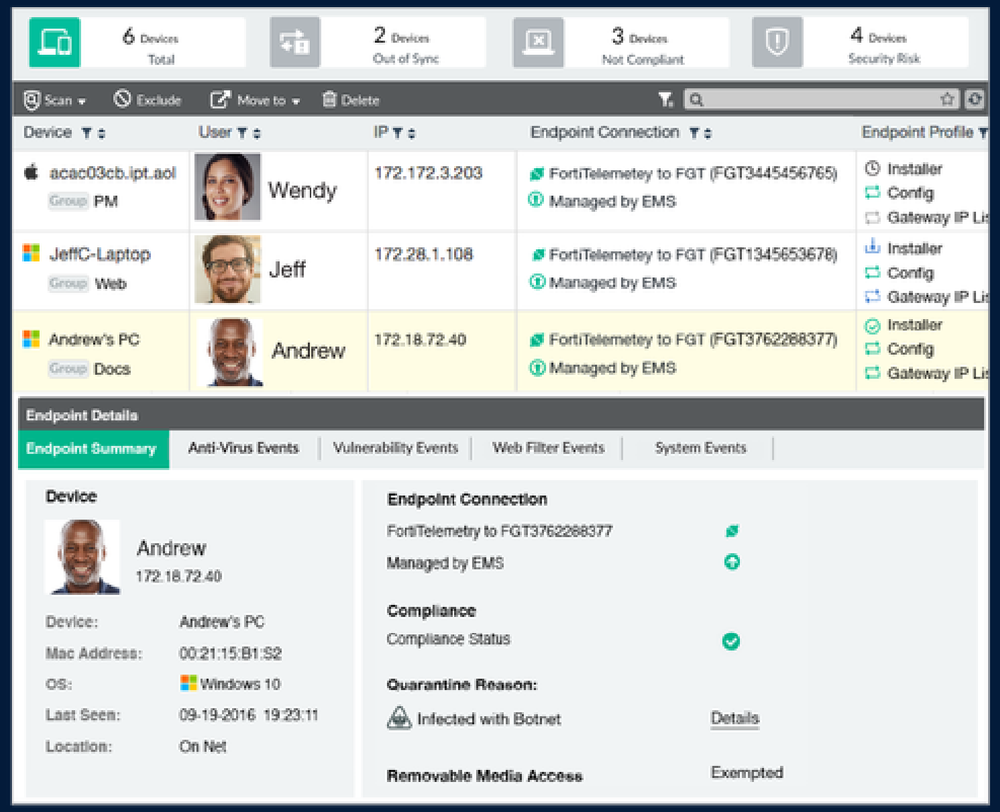
🔐 Benefits of Dial-Up IPsec VPN

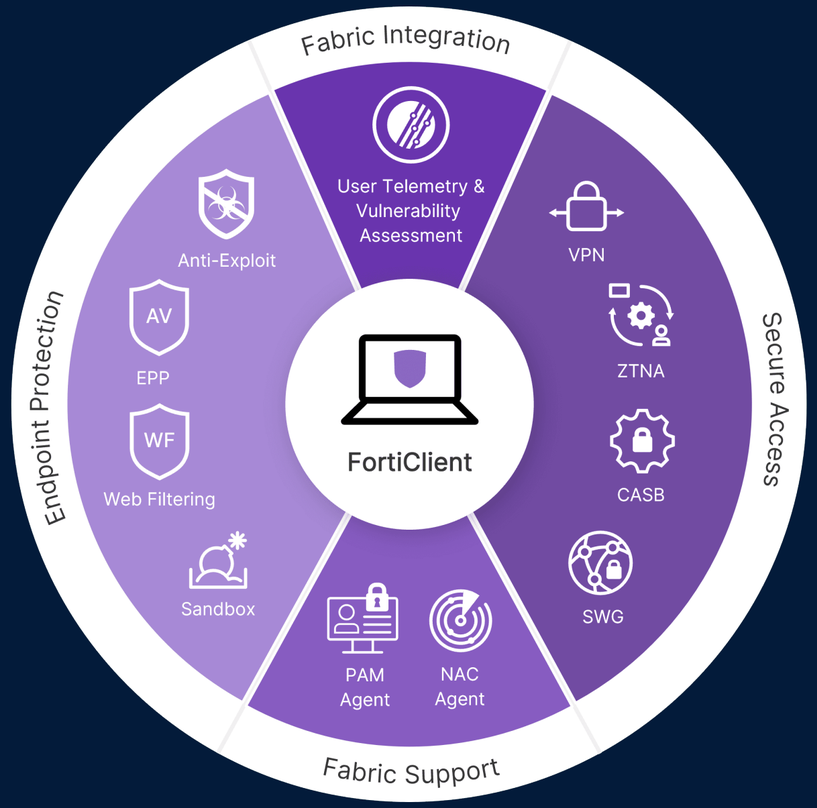
1. **Performance**
   - Generally faster throughput and lower latency since it operates at the **network layer (Layer 3)** with less overhead.
   - Good for site-to-site tunnels or power users needing heavy data transfer (file shares, VoIP, etc.).
2. **Strong Security**
   - Uses mature and well-tested cryptographic standards (IKEv2, ESP, AH).
   - Can enforce strict authentication (certificates, PSKs, EAP).
3. **Full Network Access**
   - Seamless access to the internal network as if the user is physically on-site.
   - Supports complex routing and multiple subnets easily.
4. **Scalability**
   - Widely supported across platforms, routers, and firewalls.
   - Ideal for large organizations with many remote workers or branch offices.

IntegraONE

What's next?

- Using EMS





IntegraONE

What’s next?

- Secure Access Secure Edge - SASE

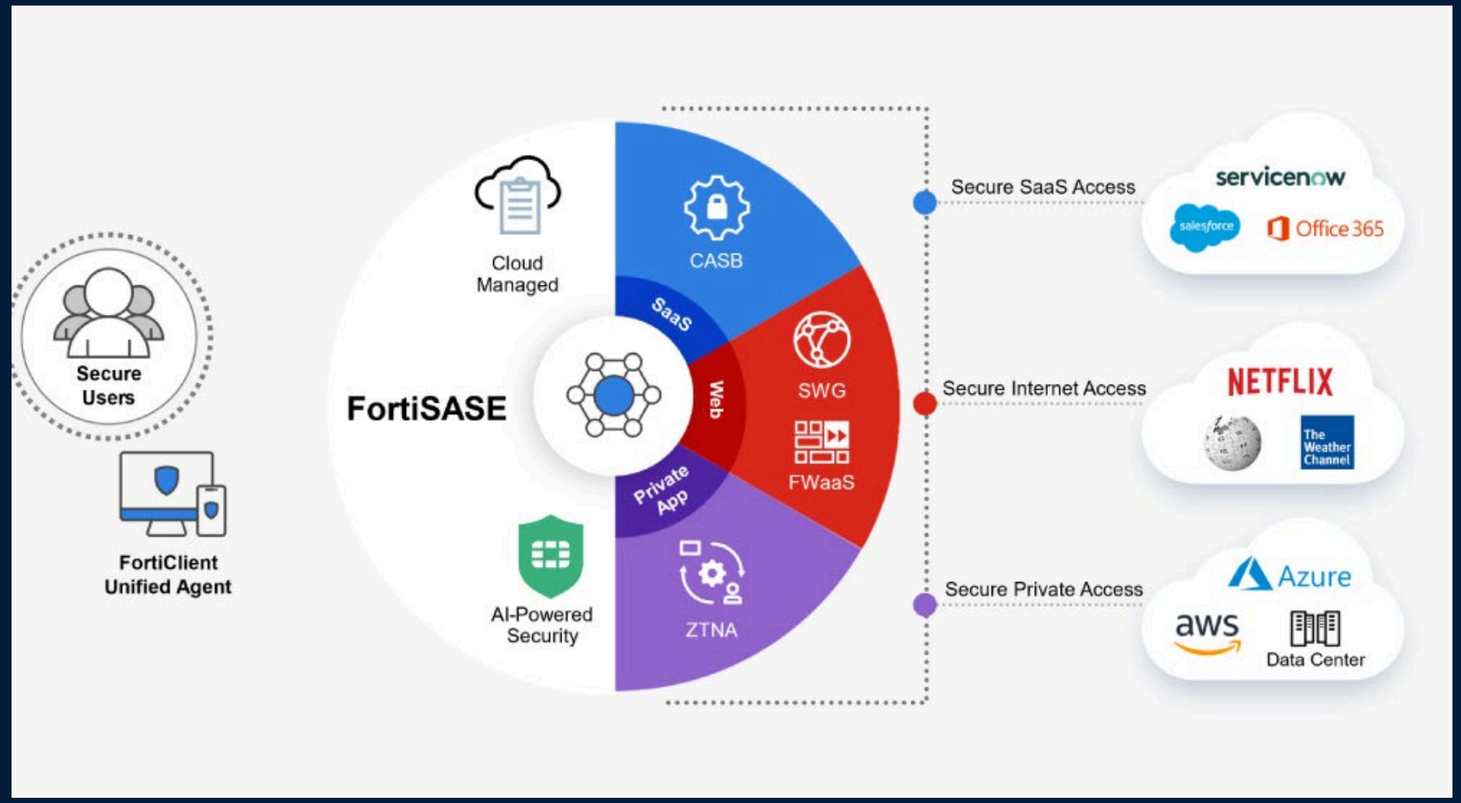
🎯 Benefits of SASE

- **Performance:** Users connect to the closest cloud edge, reducing latency.
- **Scalability:** Cloud-native, so it grows as your business grows.
- **Consistent Security:** Security policies apply everywhere (HQ, branch, remote worker, cloud).
- **Zero Trust:** Enforces identity-based access (user + device authentication).
- **Simplified IT:** Reduces need for many on-prem security appliances.

IntegraONE

What's next?

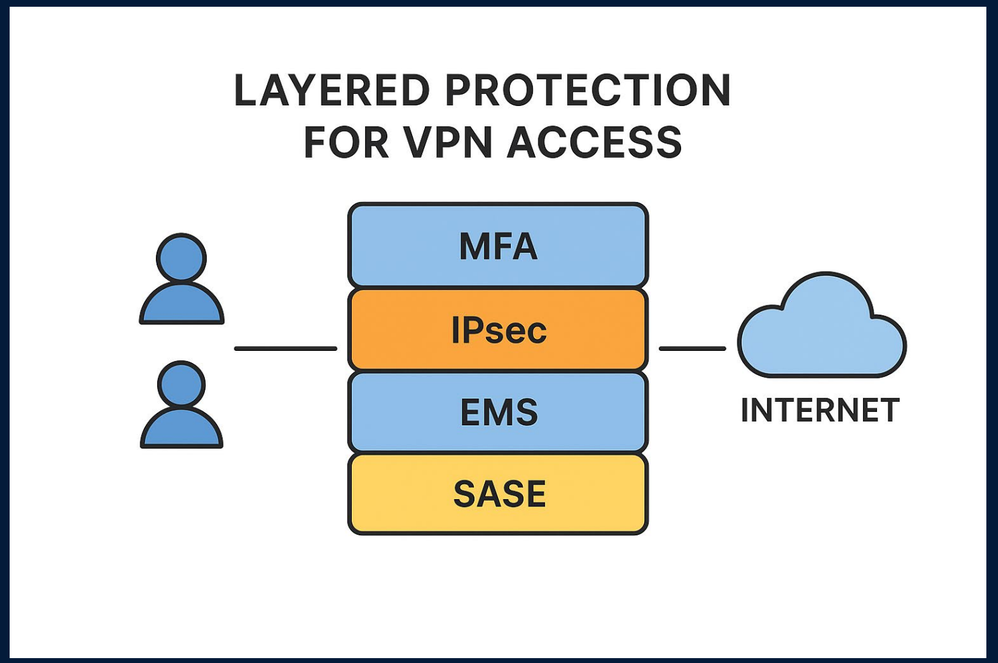
- Secure Access Secure Edge - SASE



IntegraONE

What's next?

- Time to plan for the future
  - FortiClient free VPN-only agent is being phased out
  - Creating layered protection



IntegraONE

managing
complexity
delivering

simplicity

QUESTIONS & ANSWERS

Want to ask me questions later?

adreibelbis@integraone.com
484-223-3480 ext 1266

IntegraONE

35 YEARS OF TECHNOLOGY EXCELLENCE

THANK YOU FOR BEING A PART OF OUR STORY 1990 • 2025

Thank you for attending today!

managing
complexity
delivering

simplicity