

Migrating from FortiGate SSL VPN Tunnel Mode to IPsec VPN

Key technical considerations for organizations preparing for FortiOS 7.6.3 and beyond

Table of Contents

1. Executive Summary	1
2. Why SSL VPN Migration Matters.....	2
3. SSL VPN vs IPsec VPN: Key Differences	3
4. Key Technical Migration Considerations.....	4
5. Conclusion.....	5
6. Technical Addendums.....	6

1. Executive Summary

FortiGate SSL VPN tunnel mode migration should be planned before upgrading to FortiOS 7.6.3 or later. SSL VPN tunnel mode is not available in FortiOS 7.6.3, which means organizations that still rely on this access method should review their remote access design before upgrading.

The migration is not a direct conversion from SSL VPN portals to IPsec. A new IPsec tunnel design must be created, configured, tested, and documented. The change affects endpoint client readiness, EMS licensing, IKEv2 design, NetworkID, user identification, group mapping, firewall policies, DNS, and subnet planning.

2. Why SSL VPN Migration Matters

Remote access is often treated as a utility until it fails. For organizations with distributed users, contractors, administrators, or after-hours support staff, VPN availability can directly affect operations. A rushed FortiOS upgrade can expose gaps in client versions, EMS licensing, authentication design, DNS resolution, or routing.

- SSL VPN tunnel mode is not available in FortiOS 7.6.3 and later.
- Existing SSL VPN portals and settings do not directly convert into an IPSec configuration.
- Access control shifts from SSL VPN portal assignment to group-based firewall policies and user identity.
- FortiClient and EMS requirements can affect both rollout timing and licensing.
- DNS, split tunnel or full tunnel design, and overlapping home subnets should be validated before deployment.

3. SSL VPN vs IPsec VPN: Key Differences

AREA	SSL VPN TUNNEL MODE	IPSEC VPN
FORTIOS SUPPORT	Available in FortiOS 7.6.2 and earlier.	Replacement path for FortiOS 7.6.3 and later planning.
MIGRATION METHOD	Existing SSL VPN portals and settings are already in place.	No direct conversion. A new IPsec tunnel must be designed, built, tested, and documented.
IKE VERSION	Not applicable to SSL VPN tunnel mode.	Use IKEv2 for the target IPsec deployment.
TUNNEL IDENTIFICATION	PeerID and LocalID used to identify tunnels.	Must use NetworkID to identify the tunnels.
USER ACCESS MODEL	Users roles are mapped to portals and portal-based access rules.	Access shifts to user groups, identity, and firewall policies. EAP used to identify users and apply group-based access.
CLIENT REQUIREMENTS	Free FortiClient is supported for SSL VPN tunnel mode.	FortiClient 7.4.1 minimum is required for NetworkID. FortiClient 7.4.4 or newer should be used for modern IPsec/IKEv2 planning.
EMS AND LICENSING	EMS is not required for basic SSL VPN tunnel-mode use.	EMS-licensed FortiClient 7.4.1 or later is required for modern IPsec migration because free FortiClient does not support NetworkID.
POLICY DESIGN	Access is tied to SSL VPN portal assignment.	Access must be translated into group-based firewall policy design, including split tunnel or full tunnel destinations.
DNS AND ROUTING	Existing SSL VPN DNS and route behavior known by users.	DNS suffixes, internal name resolution, route behavior, and overlapping home subnets should be validated before rollout.
ACCELERATION	SSL VPN is accelerated via same Content Processor used for inspection	IPsec VPN is accelerated in the Network processor without impact on other systems
QUANTUM	SSL VPN is not Quantum ready	Multiple Post Quantum Encryption types for IPsec keys are supported.

4. Key Technical Migration Considerations

- **Design around IKEv2:** Use IKEv2 for the replacement IPSec tunnel. From FortiClient 7.4.4 onward, IKEv1 is not supported.
- **Plan NetworkID:** For multiple dial-up IPSec tunnels, NetworkID is required to identify tunnels. PeerID / LocalID cannot be used for this purpose with IKEv2.
- **Confirm FortiClient and EMS readiness:** FortiClient 7.4.1 minimum is required for NetworkID. Free FortiClient does not support NetworkID, so EMS-licensed FortiClient is required for modern IPSec migration.
- **Rebuild access control:** SSL VPN portal roles must be translated into IPSec user groups, EAP user identification, identity selectors, and firewall policies.
- **Decide how groups will be handled:** The tunnel can be locked to a specific group, or multiple groups can be allowed on the tunnel and filtered through firewall policy identity selectors.
- **Validate transport and ports:** Confirm the required VPN transport before rollout, including ESP, UDP 500, UDP 4500 for NAT-T, and TCP 443 or custom TCP port designs where used.
- **Test DNS and routing:** Validate DNS suffix search, internal name resolution, split tunnel or full tunnel behavior, and route access before user cutover.
- **Avoid subnet overlap:** Do not use common home network ranges such as 192.168.x.x for corporate LANs where possible. Overlapping subnets can break remote-user routing and may require a remapped subnet design.

5. Conclusion

Migrating from FortiGate SSL VPN tunnel mode to IPSec VPN is manageable when it is planned early. The most important step is to treat the migration as a remote access architecture change rather than a simple VPN setting update.

Organizations should assess the current SSL VPN environment, confirm FortiClient and EMS requirements, design and pilot the IPSec replacement, and retire SSL VPN only after users and access policies have been validated.

For Technical Assistance:

INSA Integra Corp has engineers available to help you with your VPN migration needs or any other cybersecurity and networking challenges, as well as assistance with architecture, compliance, deployment or training. Reach out to us any time for assistance

-Russ Doucet



Russ Doucet, BSc, CTO
V. 613-656-0886
HQ. 55 Murray St, Suite 105 Ottawa, ON K1N 5M3
Proudly Canadian Owned & Operated

6. Technical Addendums

FortiGate CLI:

Even for those that are experienced with FortiGate and FortiClient, the SSL to VPN migration has some challenges. Following is a small collection of FortiGate CLI commands that may be relevant to your project.

set eap enable – allows identity selection request features

set eap-identity send request – activates identification prompts

(un)set authusrgrp – allows locking tunnel to one or to multiple user groups

set network-overlay enable – allows multiple networks on a tunnel via identities

Set dns-suffix-search – enables local DNS lookups through tunnel

Set remote-gw-match – allows domain match via certificate after load balancing / redirect

FortiClient Configuration:

Separately, in order to configure LDAP support on IPSec/IKEv2 tunnels, the “eap_method” in the XML must be set for “2”. This is configured in XML as follows:

```
<eap_method>2</eap_method>
```