Frequently Asked Questions

These Frequently Asked Questions and Answers provide a quick look inside how SuprNets work. For a deeper dive, explore the Technology and White Papers sections. You may also download this FAQ in its entirety…

Frequently Asked Questions		Page
1.	Why SuprNets?	2
2.	How easy is it to deploy a SuprNet?	2
3.	How does the packet Passport make trustworthy packets?	2
4.	What are the Passport's multiple rolls in the SuprStack architecture?	3
5.	Why do three layers of encryption make a difference?	3
6.	What equipment does SuprNets operate on?	3
7.	What is the SuprGate role on SuprNets?	4
8.	Do SuprNets run across all protocols and transport?	4
9.	Do SuprNets ride over the public cloud?	5
10.	How does SuprStart migrate legacy router configurations onto SuprNets?	5
11.	How do SuprMesh mutual Visas control mesh federations?	5
12.	How does SuprCloak provide transactional non-attribution?	6
13.	Are legacy security components consolidated and/or replaced by SuprNets?	6
14.	What impact does SuprNets have on the Zero Trust model (ZTNA)?	6
15.	How does SuprNets remove the need for traditional VPNs and SD-WANs?	7
16.	How does SuprNets protect against AI agents, DDoS, and general rogue attacks?	7
17.	How does the SuprNexus policy engine enforce security policies across all SuprMesh traffic?	8
18.	How do SuprNeural's AI-driven ontologies streamline policy management?	8
19.	How does SuprStack provide immediate Post-Quantum compliance without rip & replace?	8
20.	How does SuprNets defend against Harvest Now-Decrypt Later?	9

© 2026 TrustWrx, Inc. · Updated November 9, 2026

1. Why SuprNets?

The Internet is an easy crime target.

For fifty years the Internet packet has been untrustworthy. Nearly every security dollar spent tries to catch bad packets or legitimize untrusted packets from the outside – tunnels, brokers, firewalls, credential vaults, rule chains, and anti-spam – each a separate product, additional cost, another console and broader attack surface.

It is clear the security industry is fighting whack-a-mole battles with a complicated stack of outdated weapons in a war it can never win.

> *In 2027, worldwide losses to cybercrime will exceed **10% of global GDP**. The cost of the security industry fighting that problem was **more than $240 Billion in 2026**, and will be **more than $350 Billion in 2029,** most of which can be laid at the door of packets that can't be trusted. **This model is not sustainable.***

So SuprNets asked a different question –
why not make the packet itself trustworthy?
Every SuprNet packet carries its own identity, policy, provenance and routing authority inside a three-layer, cryptographic stack, with zero decryption cycles, end-to-end. SuprNets is not another component for a bloated security stack. It is an integrated ecosystem that consolidates and retires many of the legacy stack's layers – **while consolidating verifiable trust inside the packet.**

Medium: Fixing the Internet's Fundamental Flaw with Trustworthy Packets

2. How easy is it to deploy a SuprNet?

SuprStart compresses deployment from weeks to hours, or a single business day. The process is entirely graphical – zero CLI. It provisions the SuprGate, discovers and registers devices and connections, applies policy templates, connects to cloud administrative services and joins the SuprMesh – **all from a single console session**.

SuprNets may be installed across any current infrastructure. Routers, switches, firewalls, carriers, IP addressing, DNS, VPNs, applications and user workflows stay in place. At your pace, legacy network components that SuprNets subsume may by selectively retired with no effect to SuprNet operations and no restarts.

3. How does the packet Passport make trustworthy packets?

The SuprNet Passport is the world's first patented identity, security, trust and operational extension to the IP packet. It binds the verifiable identity of the packet to the unimpeachable identity of the source device – the critical trust component a standard IP header lacks.

It is a JSON bit-map assembled from locally cached SuprAdmin data for each outbound packet, and travels with the packet to its destination. Packets without a valid SuprStack encryption envelope and a Passport are silently discarded.

At every hop and endpoint, the Passport reveals to SuprStack operations who sent the packet (Source Device ID and application), which policies govern it, which federation and destination it is bound for, and which Visas authorize it.

Intermediate hops verify the Passport and the packet without decrypting the payload. **Trust therefore travels inside the packet** rather than depending on external brokers, agents or tunnels.

4. What are the Passport's multiple rolls in the SuprStack architecture?

- **Enables the SuprMesh federations** The inner encryption layers (C1 & C2) protect the packet payload, attachment and headers. The Passport sits between the middle (C2) and outer transport (C3) encryption layer. This placement lets each hop or endpoint decrypt the C3 transport layer, revealing the Passport for packet verification, policy controls, and SuprMesh Visa routing, while the payload stays encrypted inside C1 and C2.
- **Enables SuprCloak non-attribution.** The true source IP address is sequestered inside the Passport – visible only at endpoints – while the decoy sender IP address means nobody can see who is talking to whom.
- **Enables SuprNexus in-band policy management** A per packet policy digest is carried inside the Passport, providing hop and endpoint policy controls without external brokers.
- **Validates packet traffic.** External or internal packets that show up without the SuprNet encryption format, Passport and registered sender ID are rejected as defacto unwelcome, along with any rogue or imitation WireGuard session.

5. Why do three layers of encryption make a difference?

Conventional protection relies on a single encryption layer, typically TLS or IPsec. Break that one layer – through a malicious exploit, a stolen key, a lost laptop, a flawed implementation or a future quantum computer – **and the traffic is exposed.**

SuprStack wraps every packet in **three nested layers of post-quantum encryption**, each with its own set of keys that change for each packet session.

> **C1 (inner encryption)** – Encrypts the entire packet with AES-256-GCM, including payload, attachments, headers and IP addresses, producing the C1 digital blob. C1 may be bypassed for previously encrypted traffic (VPN, TLS, HTTPS, VoIP, streaming, etc.).

> **C2 (middle encryption)** – Re-encrypts the C1 blob with AES-256-GCM, using JIT per segment keys, producing the C2 blob.

> **C3 (transport encryption)** – Re-encrypts the C2 blob, while adding the Passport – all inside an independent WireGuard JIT session that opens only on traffic and is non-existent on the wire when idle.

> **Encryption keys are ephemeral and never transmitted**. Because the layers are serially dependent, an attacker would have to brute-force crack all three in proper sequence, making single-point cryptographic collapse **structurally infeasible.**

6. What equipment does SuprNets operate on?

On every platform, all elements of SuprNets operate the same way, so each device joins the same federated, policy-controlled network. Devices behind the SuprGate, including unmanaged IoT, need no endpoint software. SuprClient and SuprMobi install on laptops, smartphones,

workstations, servers and security-sensitive endpoint equipment, and connect seamlessly to the designated SuprGate.

MSPs, SMBs and commercial enterprises – Using the SuprStart graphical utility and model-specific installation packages, any off-the-shelf commercial or high-end consumer-grade router that supports OpenWrt is flashed, locally or remotely, with the SuprNet software, becoming a SuprGate.

Government and defense – The SuprStart device utility library provides the required packaging for hardened SuprGate routers and tactical edge equipment, including:

- **Land, sea and air platforms –** vehicles, vessels, aircraft and their mission systems.
- **Unmanned systems –** aerial, ground, surface and undersea drones, through SuprDrone.
- **Warfighter wearables –** body-worn and handheld devices, through SuprClient.
- **Satellite –** satellite communications terminals and ground stations.
- **Remote and forward-deployed devices –** ISR sensors, ICS/OT controllers, medical equipment and other field systems.

7. What is the SuprGate role on SuprNets?

Using the SuprStart graphical utility and model-specific installation packages, any off-the-shelf commercial or high-end consumer-grade router that supports OpenWrt is flashed, locally or remotely, with the SuprNet software, **becoming a SuprGate.**

A SuprGate is the SuprNet aggregation point for all connected wireless, wireline, IoT and other devices, including other subnet routers, switches and hubs, tunnels, daisy-chained SuprNets, and upstream and downstream addressed connections – and it brings onto the secure network all local devices with or without SuprNet endpoint software, including laptops, smartphones, drones and unmanned devices. Every SuprNet node (e.g., the doctor's office, a hospital department, a tactical force, etc.) is anchored on a SuprGate.

The SuprGate software provides the SuprStack encryption layers and SuprCloak non-attribution, enforces SuprNexus policy, supports federations over unlimited SuprMesh configurations, and calls SuprAdmin cloud services. SuprGates are provisioned graphically – no CLI – and install with minimal disruption to existing services.

8. Do SuprNets run across all protocols and transport?

Yes. On the wire, every SuprStack packet is a standard IP packet – carried in UDP, structured, routed and forwarded exactly like any other packet. Routers and firewalls handle it with no special treatment. SuprNets requires no new standards, no new RFCs and no change to existing network architecture.

SuprNets is protocol-agnostic – TCP, UDP or QUIC, over IPv4 or IPv6, encrypted or in the clear**. It is also transport-agnostic**, operating across wireless, wireline, RF, satellite, cellular, cloud and SIPRNet/NIPRNet (including AWS GovCloud). Existing VPN, TLS and SD-WAN traffic can ride inside SuprStack, or SuprStack can ride over them.

9. Do SuprNets ride over the public cloud?

There are no constraints on SuprNet connectivity. They can operate locally, across any type of connection, and freely across the public cloud with no packet payload decryption cycles end-to-end.

- **SuprMesh Federations** Under exchanged SuprMesh Visas, SuprNets and their devices may federate across any Internet infrastructure, local, cloud, public or private, encrypted or in the clear.
- **SuprMobi, SuprClient, SuprDrone** A laptop, smartphone, tactical edge device or drone is registered to a SuprNet account and SuprGate, and does not operate standalone. From anywhere in the world over any Internet connection, the device may seamlessly communicate with any federated SuprNet and device with which it holds a SuprMesh Visa pair.
- **Public Internet Traffic** Publicly destined SuprNet traffic – email, browsing, online buying, VoIP, streaming, etc. – is decrypted and handed off to the public Internet through an address proxy, keeping the SuprNet and the source device out of public view.

Concurrently, the Passport is cached at the proxy handoff, and restored to the returning traffic when it is encrypted back onto the SuprNet, applying SuprNexus restrictive policies to both the outbound and the returning public traffic.

10. How does SuprStart migrate legacy router configurations onto SuprNets?

SuprStart is the SuprNet's graphical onboarding and provisioning tool – zero CLI. For new networks or live conversions, it detects and graphically transfers the new or prior router and device configuration onto the SuprGate with minimal interruption, with no command-line expertise required. The previous router may be left in place, removed, or deprecated over time without a restart or disruption of operations..

In the same workflow, SuprStart provisions the gateway, registers devices, applies policy templates, completes the first gateway-to-cloud key exchange and joins the SuprMesh. Deployment that typically takes weeks is compressed to hours or a single business day – **all from a single console session**.

Every SuprNets management function is graphical. From there, policy and federation are managed through SuprAdmin, SuprNexus and SuprMesh, replacing CLI-driven rule maintenance with visual, role-scoped authoring.

11. How do SuprMesh mutual Visas control mesh federations?

SuprMesh federation runs on two credentials. The Passport carries the origin's asserted identity, policies and mesh credentials – **Visas travel with the Passport, carrying the permissions a destination grants.** Any federation requires two mutually exchanged Visas – each party grants the other explicit, scoped access.

Each Visa defines its owner and holder, the devices and apps allowed, packet behavior and management dates and times. Visas are authored graphically, and each packet's Passport carries the Visas that authorize it, so mesh node traffic is enforced in-band, with no central control plane or out-of-band lookups.

A Visa or its devices can be paused, modified or quarantined in one click with zero impact on uncompromised peers. Because enforcement travels in each packet, trust continues under denied, disrupted, intermittent or limited (DDIL) connectivity.

12. How does SuprCloak provide transactional non-attribution?

Today, every standard packet exposes its sender's address – the first input to malicious targeting. SuprCloak breaks the link between a transaction and its source, meaning **nobody can see who is talking to whom.**

Before a packet leaves its source, SuprCloak replaces the true source address with a **Decoy Anchor** – a real, network-owned IPv6 address used only for SuprNet traffic and never configured on any interface. By removing the sender's true IP address from the public path, SuprCloak provides true transactional confidentiality across federations, **meaning no one can link any sender to any recipient** – the forward path conceals which device is sending, the return path conceals which gateway is answering, and the Passport privately holds the addressing the other needs.

The true IP address is sealed inside the protected Passport and revealed to SuprStack operations only at the destination to inform returning traffic. **Decoy-addressed traffic is hostile by definition and dies at the upstream router.**

13. Are legacy security components consolidated and/or replaced by SuprNets?

SuprNets consolidates firewall, VPN concentrator, SD-WAN controller, ZTNA gateway and IoT manager functions into one platform-neutral system.

The Packet Passport, carried in every packet, along with the SuprNexus policy engine, functionally subsumes VPN, TLS/PKI, ZTNA brokers, IAM/PAM, policy decision point (PDP) services, SD-WAN policy, federation trust brokers, application-layer ACLs and network access control (NAC).

Consolidation is on your schedule, not a prerequisite. At deployment, existing VPN, TLS, SD-WAN and Zero Trust investments keep their roles. Once traffic rides SuprStack, legacy categories – VPN concentrators, ZTNA and IAM/PAM brokers, overlay policy engines – can be retired at the pace you choose. Routers, switches, carriers and path firewalls continue to forward SuprStack traffic unchanged.

14. What impact does SuprNets have on the Zero Trust model (ZTNA)?

The Zero Trust (ZTNA) principle – never trust, always verify – is sound, but today's implementations verify at the session or application level through external brokers and policy decision points, and most still operate across VPNs. Each adds latency, a console, more cost and a point of failure, and enforcement degrades when those services are unreachable.

SuprNets move Zero Trust to the packet layer. Every packet carries its own identity and policy in its Passport, so verification happens on every packet, at its origin, at every hop and at its destination – with no runtime calls to external policy services. **Policy is keyed to permitted relationships, mission intent and mesh behavior rather than network topology** – not IP addresses, iptables and ports.

SuprNets aligns with all seven pillars of the DoD Zero Trust Reference Architecture v2.0 and meets NIST SP 800-207 core tenets at the packet layer. It also delivers the containment model NSA prescribes for the Zero Trust network pillar – one-action quarantine by Device ID while the network keeps operating. Existing Zero Trust investments keep their role until you choose to retire them.

Medium: Zero Trust – a Doctrine Without Deliverance

15. How does SuprNets remove the need for traditional VPNs and SD-WANs?

VPNs build persistent point-to-point tunnels to protect traffic between sites – SD-WANs add an overlay to steer them. **Both protect the path, not the packet**, and both add administrative overhead and attack surface. And, handing off traffic between VPNs means the exposure of decryption and re-encryption cycles.

SuprNets protect every packet directly – end-to-end. Three-layer per-packet JIT encryption across SuprMesh replaces the point-to-point tunnel – no persistent tunnels, no manual key or certificate management – and policy, routing authority and federation travel in-band in each packet's Passport. SuprStack consolidates VPN concentrator and SD-WAN controller functions, and SuprMesh Visas federate sites across any transport without a central control plane.

SuprNets does not force removal. Existing VPNs and SD-WANs can stay in place – SuprStack can carry their traffic inside it or ride over them. Once traffic rides SuprStack, VPNs and overlay policy engines can be retired on your schedule, with zero impact on the active SuprNet.

16. How does SuprNets protect against AI agents, DDoS, and general rogue attacks?

On a SuprNet, only traffic from registered devices is legitimate. All other traffic is defacto rogue. SuprNets defends against everything that reaches the SuprStack – including direct port attacks, application-layer (L7) and paced DDoS floods, general rogue traffic, and the AI-driven intrusion, malware and reconnaissance it carries.

> **Silence to strangers** – Any rogue attack dies at the port. All packets without a valid SuprStack encryption session and Passport receive no reply, reset or error. Scanners and AI reconnaissance agents see nothing, and a silent destination cannot serve as a reflector.

> **Forged sources** – Each outbound source IP address is matched to the device's registered IP address at origin – mismatches are dropped silently – stopping lateral forged-source floods and internal reflection.

> **DDoS floods** – per-device rate tracking in the gateway kernel drops or throttles traffic above policy thresholds.

> **Compromised endpoints** – SuprNexus blocks call-home, lateral movement and disguised file types, and binds internet and AI-service access to registered applications.

> **Containment** – every packet is attributable by device, and one action quarantines a device at machine speed without affecting other resources.

> ***Note:*** *Volumetric DDoS floods large enough to saturate the access link are a carrier-level problem and outside SuprNets' scope.*

17. How does the SuprNexus policy engine enforce security policies across all SuprMesh traffic?

SuprNexus is a kernel-resident policy engine that replaces the IP-address-and-port model of traditional iptables firewall rules with **policy keyed to permitted relationships, tactical intent and intended behavior** – eliminating CLI rule chains and reload drops. Policies are authored and managed graphically, and role-scoped, while updates propagate near-instantly without Gateway restarts.

Policies are held in an in-memory bit-mapped matrix, delivering constant-time lookups regardless of policy count across OSI Layers 2 through 7. Rules span device, user, application function, page, URL, file type, protocol, time window, mesh node and federation, and more.

Because a SuprNexus policy digest travels in each packet's Passport and is enforced locally on gateways and endpoints, SuprNexus applies consistent rules across all SuprMesh traffic with no runtime calls to external PAM/IAM policy services. It enforces per-application egress, a designated DNS resolver and a default-deny allowlist of true file types, domain names, email addresses and more.

18. How do SuprNeural's AI-driven ontologies streamline policy management?

SuprNeural is an AI and ontology engine. It observes multiple aspects of mesh traffic patterns using supervised machine learning enriched by Basic Formal Ontology and Common Core Ontologies (BFO/CCO).

From those observations, SuprNeural recommends policy to operators through a review-and-approve loop, streamlining policy management – refinement is driven by observed relationships and behavior, and operators approve rather than author from scratch.

19. How does SuprStack provide immediate Post-Quantum compliance without rip & replace?

The US Government and Department of War (DoW) PQC Strategy requires all systems to support post-quantum cryptography by 2030 and use it by 2031. The conventional path – rewriting buried crypto calls inside thousands of legacy applications and tunnels – **is not achievable at cost or on schedule.**

SuprNets seals all traffic inside the three-layer SuprStack at the packet layer. Legacy application crypto, VPNs and TLS stay untouched. Effort scales with SuprNets installed, not applications updated – one gateway protects every device, tunnel and system behind it in transit – one app or ten thousand, modern or forty years old, encrypted or not.

Immediate compliance is by construction. Current NIST standards presume a single layer of cryptography and measure compliance by approved algorithm. SuprStack's **quantum resistance is by architectural construct and crypto-independent** – resting on three ephemeral, never-transmitted keys that would have to be cracked in proper serial sequence. Even though the outer WireGuard C3 layer is not NIST-approved for PQC compliance, the inner two layers of AES-256 achieve NIST FIPS-197 compliance for all traffic.

On that basis, PQC and HNDL protection is immediate for all traffic riding SuprStack. NIST PQC Algorithm-level alignment with NIST PQC, CNSA 2.0 and FIPS 140-3 is on the company's roadmap, contingent on a government contract.

20. How does SuprNets defend against Harvest Now-Decrypt Later?

In a harvest-now-decrypt-later (HNDL) attack, adversaries capture encrypted traffic today and store it until a future quantum computer can break it.

SuprNets defeats HNDL through the complexity of the three-layer SuprStack, not through any single algorithm. Each packet is protected by three independently keyed layers – keys are ephemeral, never transmitted and erased after use – the inner key when its packet is first encrypted, the middle key for the second layer of encryption, and the outer key when the packet is encrypted for transmission. To recover a payload, an attacker would have to crack multiple keys in proper sequence.

Because this protection derives from the architecture rather than solely on the crypto employed, it applies the moment traffic rides SuprStack, with no near-term crypto updates to applications or tunnels, while algorithm upgrades proceed at a manageable pace.