CERTES
CERTESNETWORKS.COM

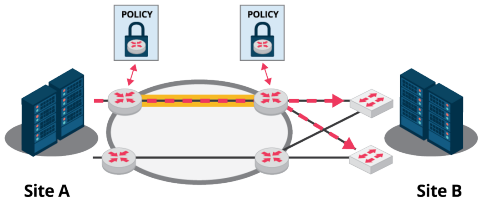
SOLUTION NOTE

The Zero Trust WAN Difference

Certes Networks **Zero Trust WAN (ZTWAN)** is an innovative security policy and encryption key management solution providing scalable network-wide encryption. By providing global control of the generation of policies and dynamic distribution of keys, ZTWAN enables organizations to encrypt data transmissions over any type of network without compromising application or network performance. ZTWAN introduces three areas of improvement over traditional IPsec for network-wide encryption deployments: group policy definition, dynamic traffic flow and encryption without tunnels.

Group Policy Definition

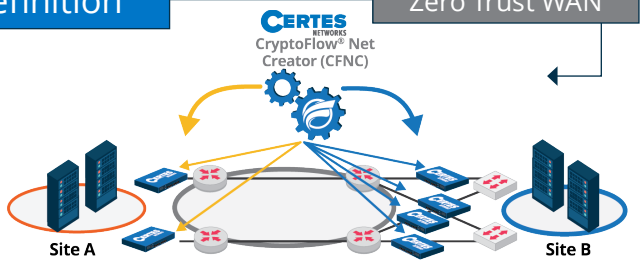
Traditional IPsec



Traditional IPsec policies are strictly device oriented

- ✓ This requires encrypted traffic be routed from a specific device to another specific device.
- ✓ The result is static tunnels across the network.

Zero Trust WAN

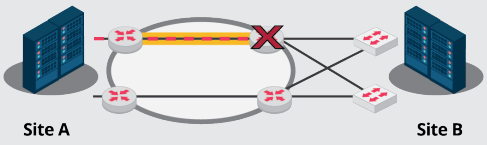


With **ZTWAN** policies are network oriented, not device specific.

- ✓ The encryption keys are distributed to groups of endpoints, so any group member can talk to any other.
- ✓ This allows any-to-any communication without the point-to- point constraints of tunnels.

Dynamic Traffic Flow

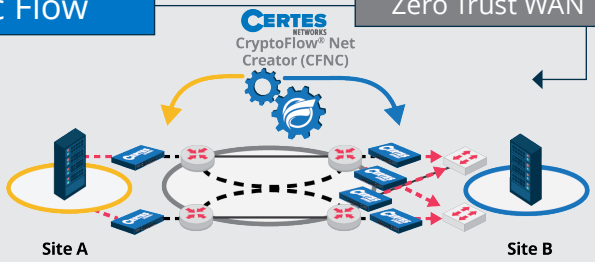
Traditional IPsec



Traditional IPsec requires encrypted traffic be routed from a specific device to another specific device.

- ✓ If a router goes down, the data cannot be decrypted without being re-transmitted.
- ✓ The result is the inability to route traffic around congestion.

Zero Trust WAN

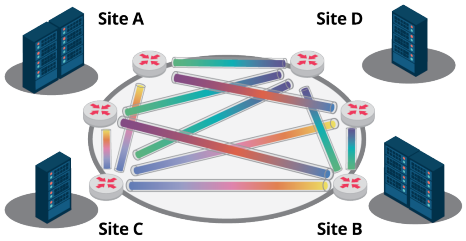


With **Certes Enforcement Points (CEP)**, the original header is preserved.

- ✓ CEP groups and shared keys enable secure load balancing.
- ✓ The result is encrypted data traveling the most efficient route to the destination site.

Encryption without Tunnels

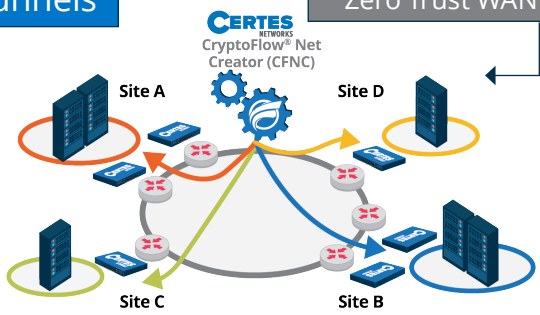
Traditional IPsec



Traditional IPsec requires additional tunnels for new sites

- ✓ Complexity increases exponentially as static tunnels are added
- ✓ The result is a complex and static routing cloud on top of a flexible and dynamic network

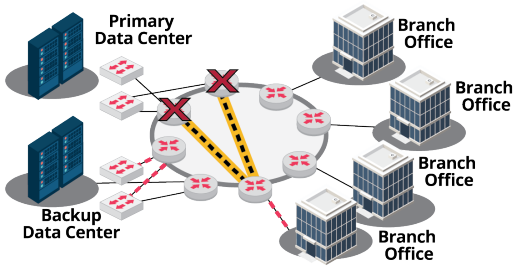
Zero Trust WAN

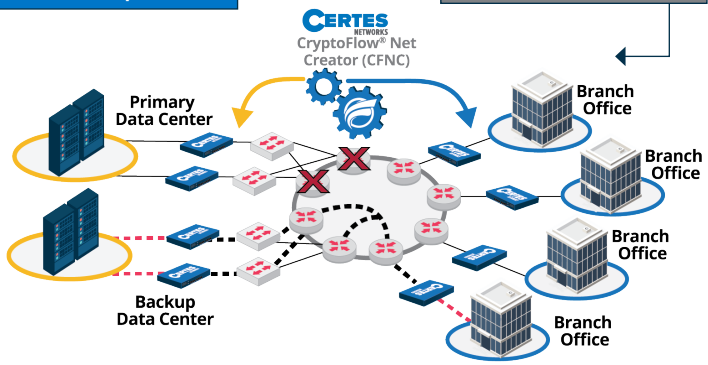


The **ZTWAN** solution encrypts data without disrupting network operations or application performance

- ✓ Additional sites are easily added using site-based policies
- ✓ The result is a scalable, flexible, dynamic and secure network

Traditional IPsec — Redundant Hub & Spoke — Zero Trust WAN





VPNs require static **IPsec tunnels.**

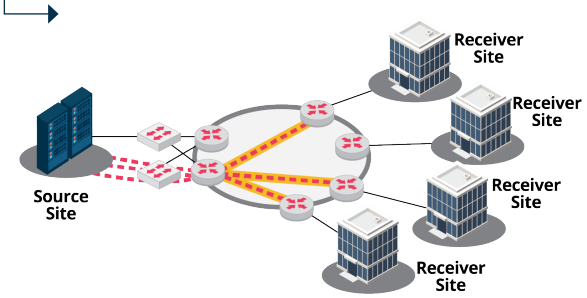
- ✓ IPsec tunnels require pre-determined paths for encrypted data, which negates load balancing.
- ✓ In the event of a primary data center failure, traffic must be resent to the back-up site.
- ✓ The result is unnecessary complexity, loss of load balancing and delayed failover with the risk of packet loss.

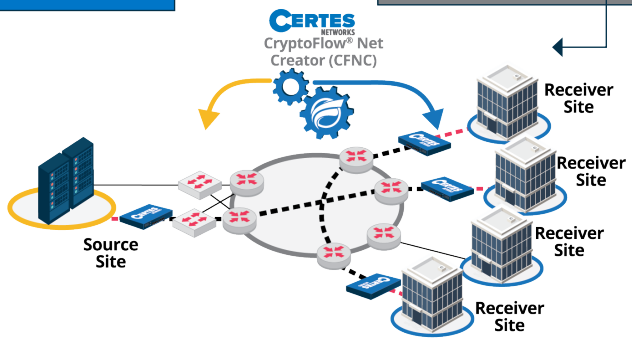
With a **ZTWAN** hub and spoke policy, all sites are defined and grouped as hub or spoke sites.

- ✓ All devices in a group are given a common group encryption key.
- ✓ Grouping enables hot failover without down time or packet loss.
- ✓ The result is an encrypted network that routes and performs services as normal in the event of a failure.

ZTWAN group policy definition, dynamic flow of encrypted traffic and encryption without tunnels combine to enable simplified network-wide encryption deployments for redundant hub and spoke networks, multicast applications and any other network, regardless of size, type or topology.

Traditional IPsec — Multicast Applications — Zero Trust WAN





With **IPsec VPNs**, traffic must be routed from a specific device to another specific device.

- ✓ Data streams must be replicated to each device before entering the static tunnel.
- ✓ The result is excessive traffic congestion and network performance degradation.

A **ZTWAN** multicast policy defines source and receiver sites.

- ✓ All devices in a multicast group are given a common group key.
- ✓ Encryption is wire-speed and does not disrupt latency-sensitive applications.
- ✓ The result is encrypted multicast transmissions without data stream replication or network changes.

About Certes

Certes Networks Zero Trust Security solutions protect data and applications in motion with a range of software defined security solutions. Our Zero Trust framework protects application traffic over any environment to any user, device or location; all this without affecting network or application performance whatsoever. Our patented and industry leading layer 4 stealth encryption solution gives you "Encryption without Compromise". **For more information visit CertesNetworks.com.**

Certes Networks Headquarters
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108
Tel: 1 (888) 833-1142
Fax: 1 (412) 262-2574
CertesNetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
sales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
sales@certesnetworks.com

Europe, Middle East & Africa Sales
emea@certesnetworks.com

V1-04-26-2017