VPN and IPSec Overview

Steven Moran
TECHNICAL INSTRUCTOR

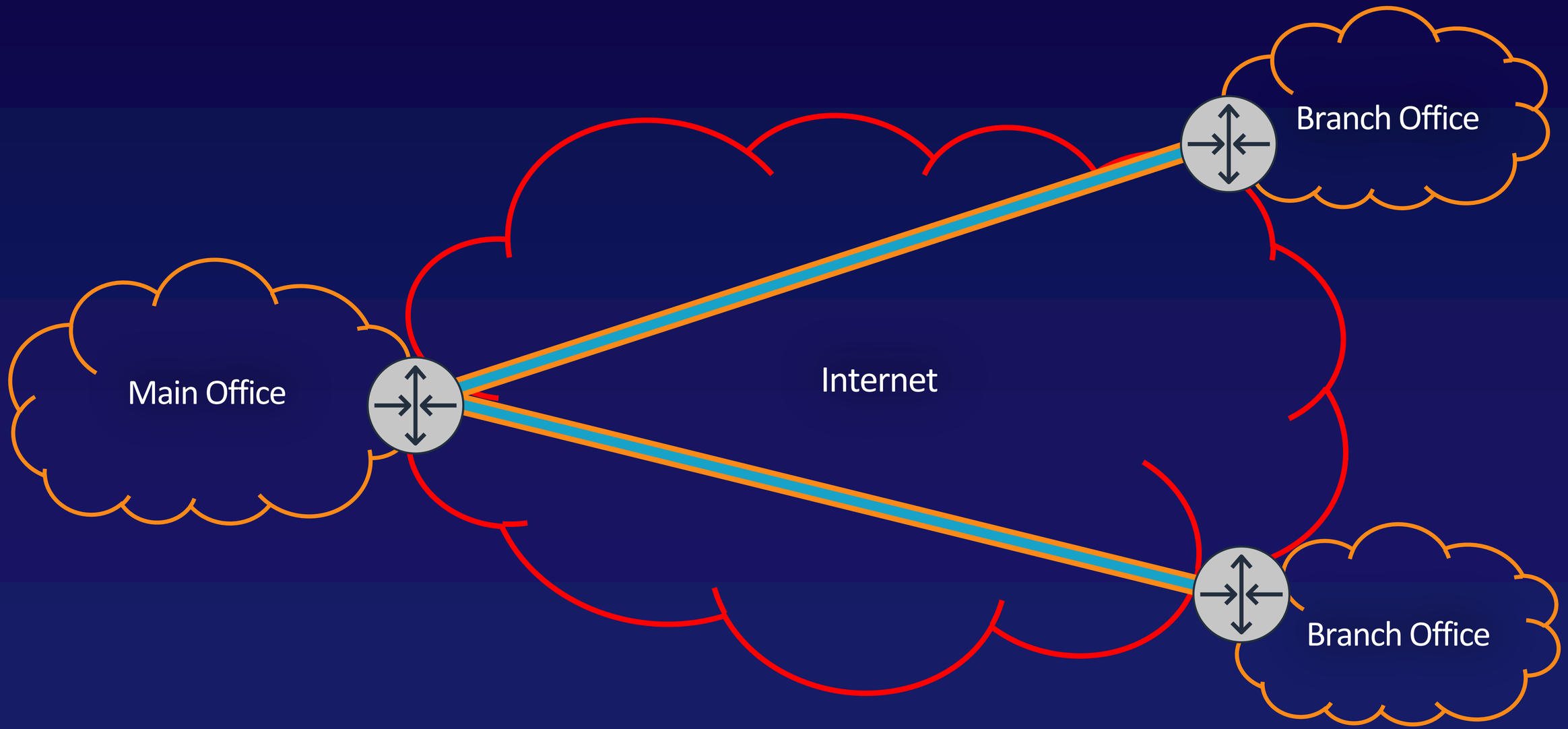
What's a VPN?

Virtual Private Network

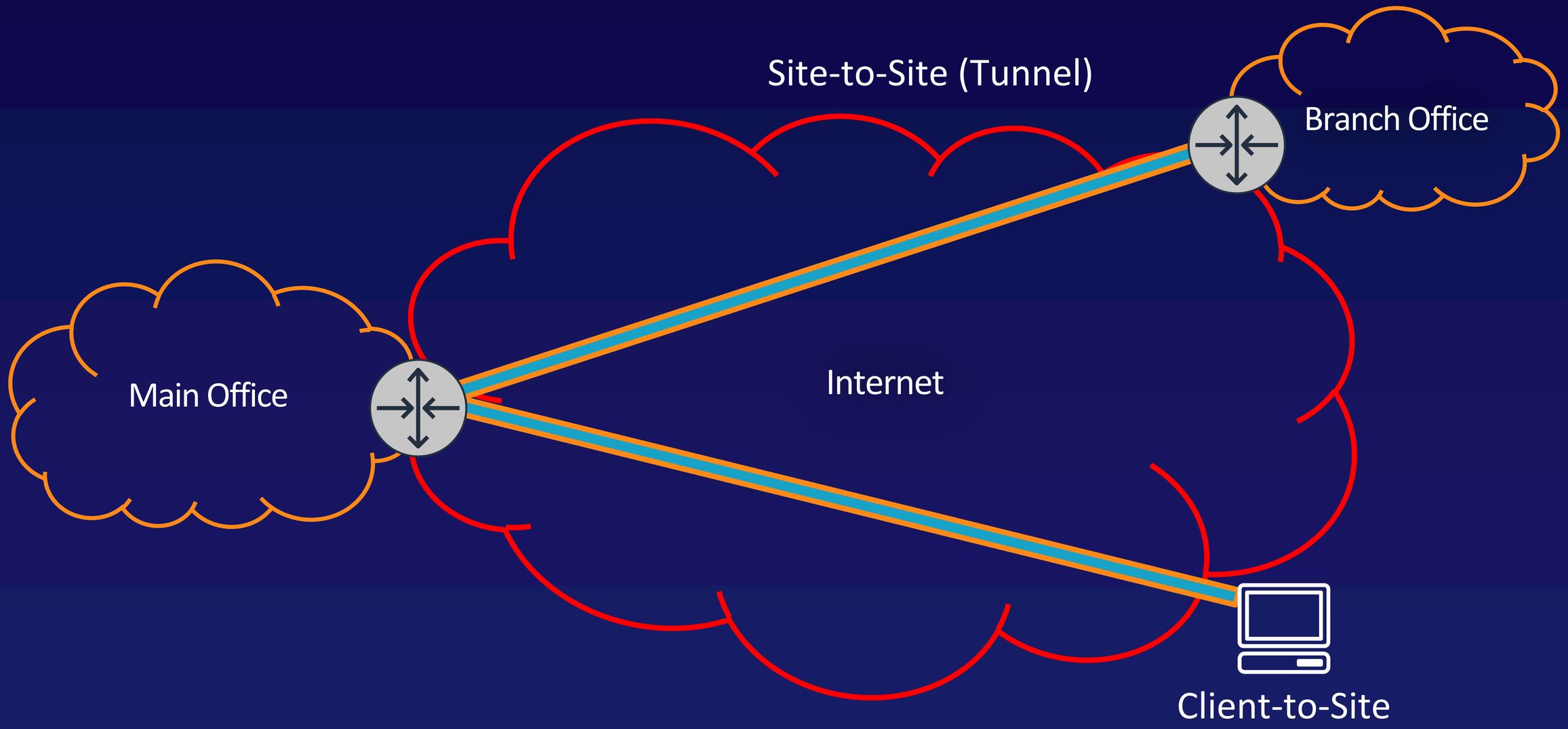
A secure, logical network connection
on top of less-secure,
physical network infrastructure.

Private traffic is protected by a
VPN protocol.

What's a VPN?



What's a VPN?



Establishing an IPSec Tunnel

VPN endpoint systems on each network must be pre-configured.

- Identity of other endpoint
- Shared authentication method
- Security policies
- “Interesting” traffic (Policy-based or Route-based)

Establishing an IPSec Tunnel

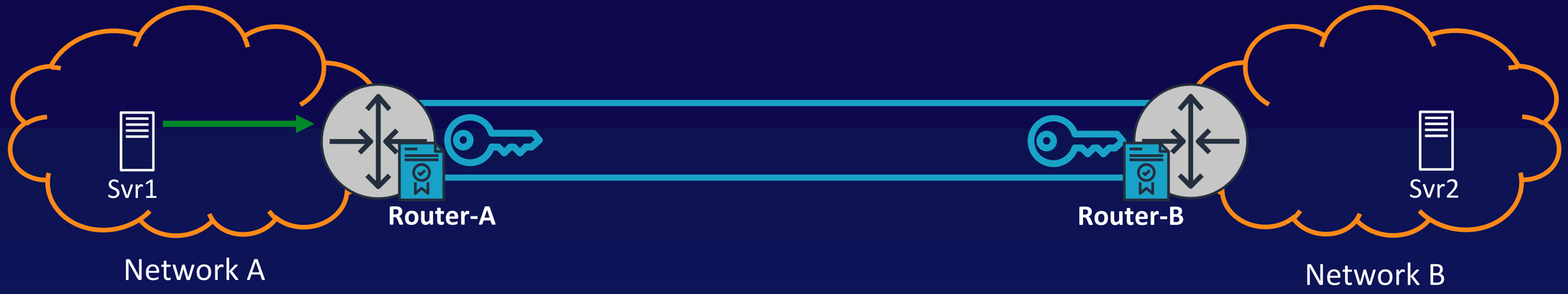
1. “Interesting” traffic is detected by local endpoint

Establishing an IPSec Tunnel

1. "Interesting" traffic is detected

2. Internet Key Exchange (IKE) phase 1
   - Also referred to as "Main Mode"
   - Negotiate a security policy for key exchange
   - Perform the key exchange (Diffie-Hellman)
   - Mutually encrypted authentication

Establishing an IPSec Tunnel

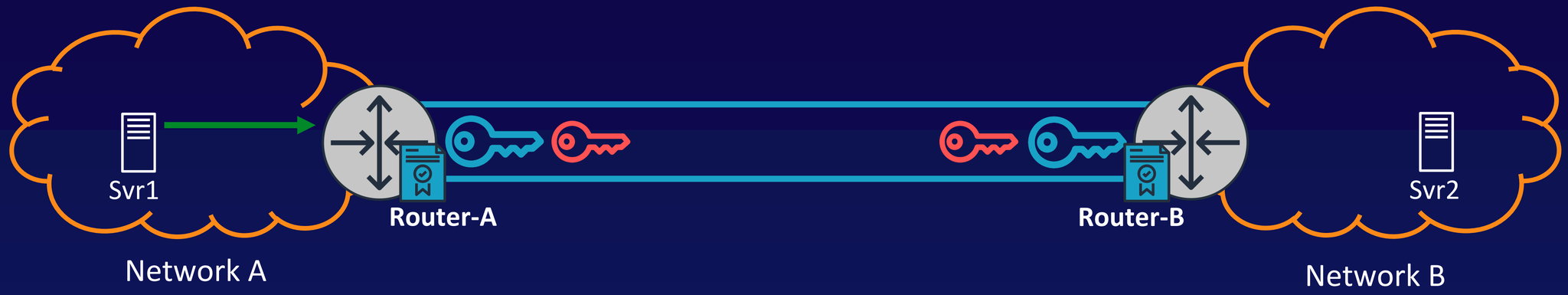


Phase 1 Tunnel

A single, two-way IKE security association between IPSEC peers

1. "Interesting" traffic is detected
2. Internet Key Exchange (IKE) phase 1

Establishing an IPSec Tunnel

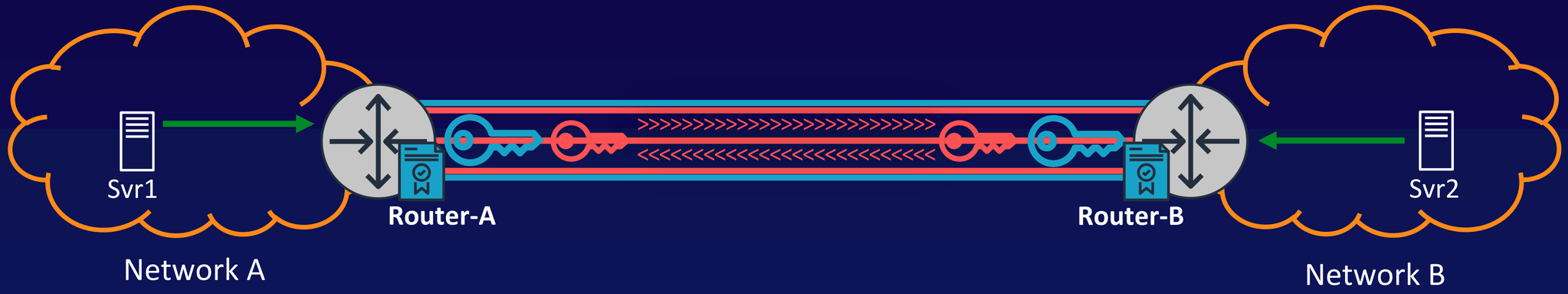


Phase 1 Tunnel

A single, two-way IKE security association between IPSEC peers

1. "Interesting" traffic is detected
2. Internet Key Exchange (IKE) phase 1
3. IKE phase 2 (IPSec)
   - Also referred to as "Quick Mode"
   - Peers do NOT re-authenticate
   - Protected traffic is identified
   - Generate or refresh keys

Establishing an IPSec Tunnel



Phase 1 Tunnel

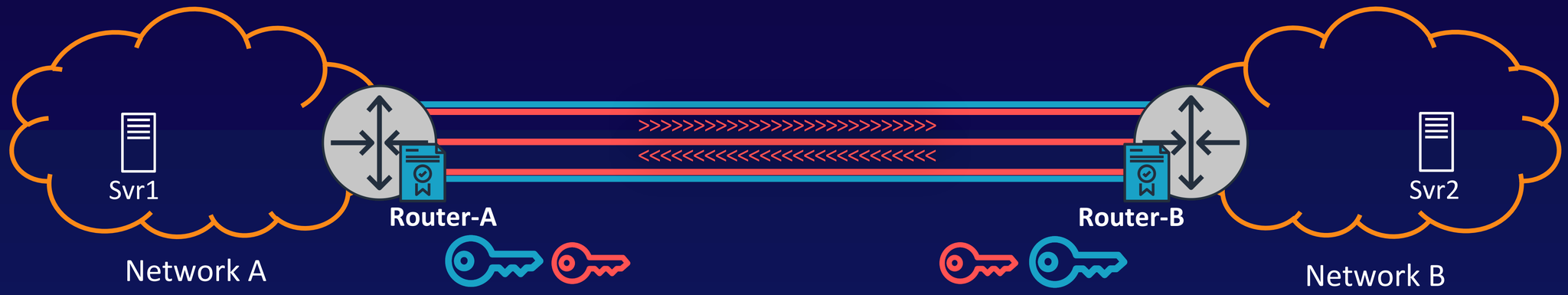
A single, two-way IKE security association between IPSEC peers

1. "Interesting" traffic is detected
2. Internet Key Exchange (IKE) phase 1
3. IKE phase 2 (IPSec)
4. IPSec tunnel is established

Phase 2 Tunnel

Two, one-way IPSec security associations between networks

Establishing an IPSec Tunnel



Phase 1 Tunnel

A single, two-way IKE security association between IPSEC peers

1. "Interesting" traffic is detected
2. Internet Key Exchange (IKE) Phase 1
3. IKE Phase 2 (IPSec)
4. IPSec tunnel is established
5. IPSec tunnel is terminated

Phase 2 Tunnel

Two, one-way IPSec security associations between networks

What's a security association?

A relationship where all parties share the same security settings

Traffic that requires different security settings would require its own security association.

VPNs using multiple security policies will need to support multiple security associations.

Security Associations

Security associations are controlled by the type of VPN being configured:

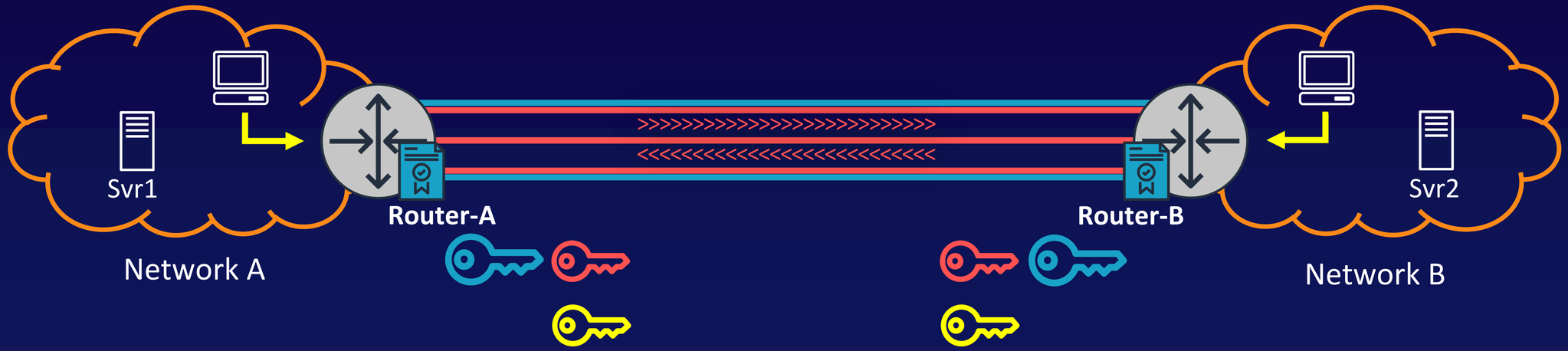
Policy-based

- *Admin-configured rule sets define VPN-permitted traffic and security settings.*
- *One security association created per matched rule set.*

Route-based

- *Traffic must target destination network to use VPN.*
- *Only a single security association is created for all traffic.*

Security Associations: Policy-based VPN



Phase 1 Tunnel

A single, two-way IKE security association between IPSEC peers

Phase 2 Tunnel

Two, one-way IPSec security associations between networks

Security Associations: Policy-based VPN

Phase 1 Tunnel

A single, two-way IKE security association between IPSEC peers

Phase 2 Tunnel

Two, one-way IPSec security associations between networks

Phase 2 Tunnel

Two, one-way IPSec security associations between networks

AWS Site-to-Site VPN Connections

- The IPSec process for an AWS Site-to-Site VPN connection is identical.
- Tunnels are only established by traffic flowing from on-prem to AWS – never the other direction!
- AWS VPN tunnels can only support a single pair of IPSec security associations.

Fast Takeaways

VPNs logically isolate and secure private traffic while using untrusted infrastructure.

VPNs are useful where persistent network connections are not needed or are too expensive.

VPN performance is limited by the quality of the traffic path across the existing infrastructure.

AWS Site-to-Site VPN Connections only support IPv4 and IPSec.