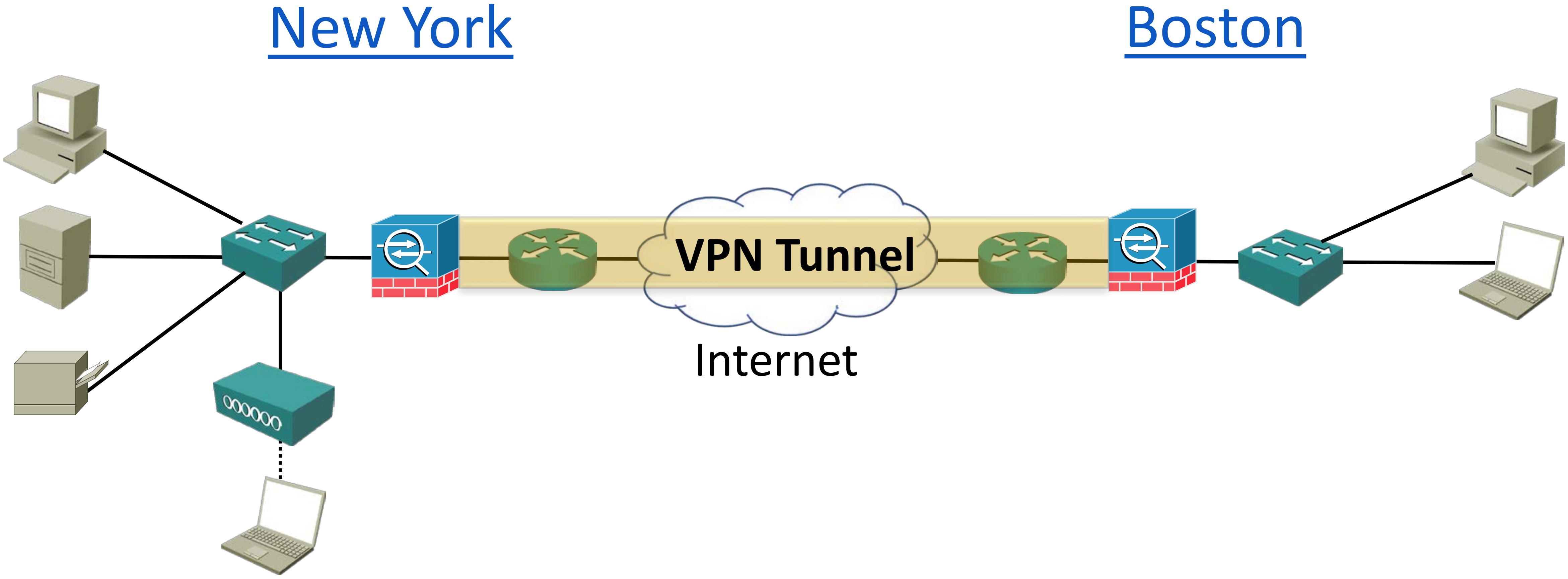
Site-to-Site VPNs



FLACKBOX
www.flackbox.com

Site-to-Site VPNs

- Site-to-Site VPNs use symmetric encryption algorithms such as DES, 3DES and AES to send encrypted traffic between locations over an untrusted network such as the Internet
- Traffic inside an office is often unencrypted as it is seen as a trusted network
- VPN tunnels can however also be deployed internally
- Cisco TrustSec is another solution for internal authentication and encryption

Site-to-Site VPNs

- Site-to-Site VPN tunnels typically terminate on a firewall or router on both sides
- A pre shared key can be configured on both sides of the tunnel or certificates can be used
- Certificates offer a more scalable solution

IPsec

- IPsec is a framework of open standards that provides secure encrypted communication an IP network.
- Internet Key Exchange (IKE) handles negotiation of protocols and algorithms, and generates the encryption and authentication keys
- Internet Security Association and Key Management Protocol (ISAKMP) defines the procedures for authenticating and communicating peer creation and management of Security Associations. It typically uses IKE for key exchange.
- IKE and ISAKMP are sometimes used synonymously.

IPsec

- Authentication Header (AH) provides integrity, authentication and protection from replay attacks
- Encapsulating Security Payload (ESP) provides confidentiality, integrity, authentication and protection from replay attacks
- ESP is more commonly used

ESP Tunnel Mode

- Tunnel mode protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by another set of IP headers.
- It is widely implemented in site-to-site VPN scenarios.

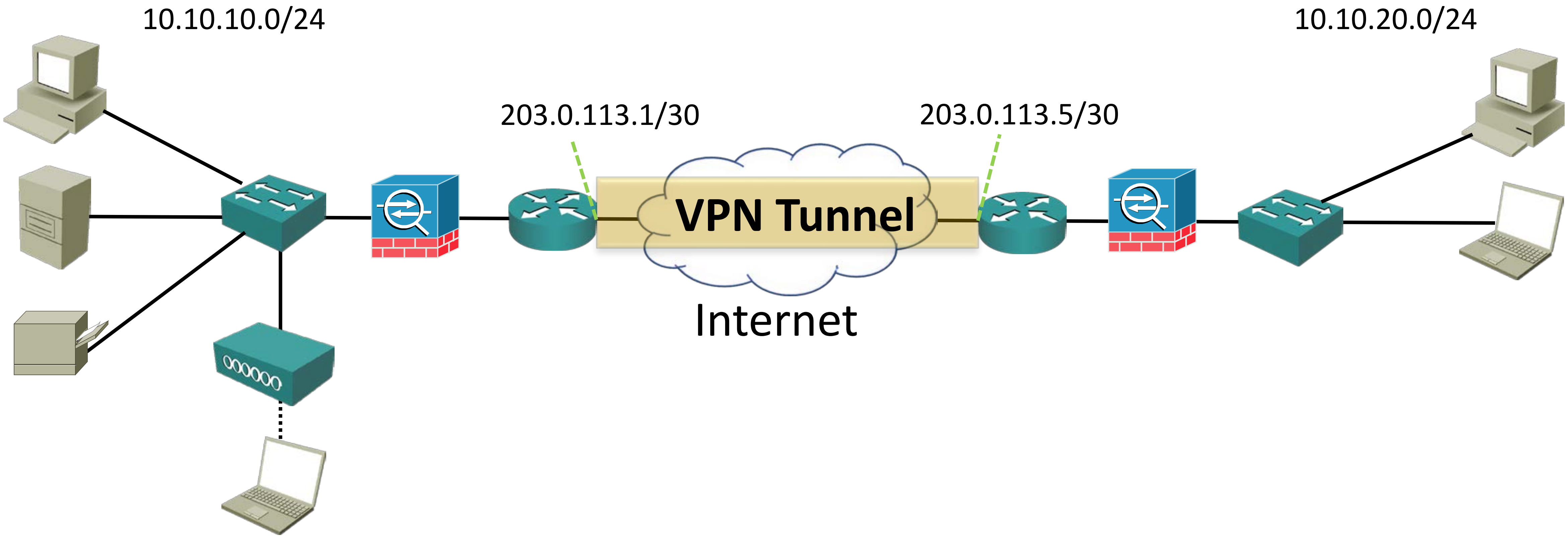
ESP Transport Mode

- The transport mode encrypts only the payload and ESP trailer; so the IP header of the original packet is not encrypted.
- The IPsec Transport mode is implemented for client-to-site VPN scenarios.
- The transport mode is usually used when another tunneling protocol (such as GRE, L2TP) is used to first encapsulate the IP data packet, then IPsec is used to protect the GRE/L2TP tunnel packets.

IPsec VPN Implementation

- Interesting traffic: The VPN devices recognize the traffic to protect.
- ISAKMP / IKE Phase 1: The VPN devices negotiate an IKE security policy, authenticate each other and establish a secure channel.
- ISAKMP / IKE Phase 2: The VPN devices negotiate an IPsec security policy to protect IPsec data.
- Data transfer: The VPN devices apply security services to traffic, then transmit the traffic.

IPsec VPN Configuration



Phase 1

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#crypto isakmp key Flackbox address 203.0.113.5
```

ACL to Define Interesting Traffic

```
R1(config)#ip access-list extended FlackboxVPN-ACL
R1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255
10.10.20.0 0.0.0.255
```

Phase 2

```
R1(config-ext-nacl)#crypto ipsec transform-set FlackboxTS
esp-aes esp-sha-hmac

R1(config)#crypto map FlackboxCM 10 ipsec-isakmp
R1(config-crypto-map)#set peer 203.0.113.5
R1(config-crypto-map)#set transform-set FlackboxTS
R1(config-crypto-map)#match address FlackboxVPN-ACL

R1(config-crypto-map)#interface Serial0/1/0
R1(config-if)#crypto map FlackboxCM
```

Exclude VPN Traffic from NAT ACL

```
R1(config)#ip access-list extended FlackboxNAT-ACL
R1(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255
10.10.20.0 0.0.0.255
R1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
```