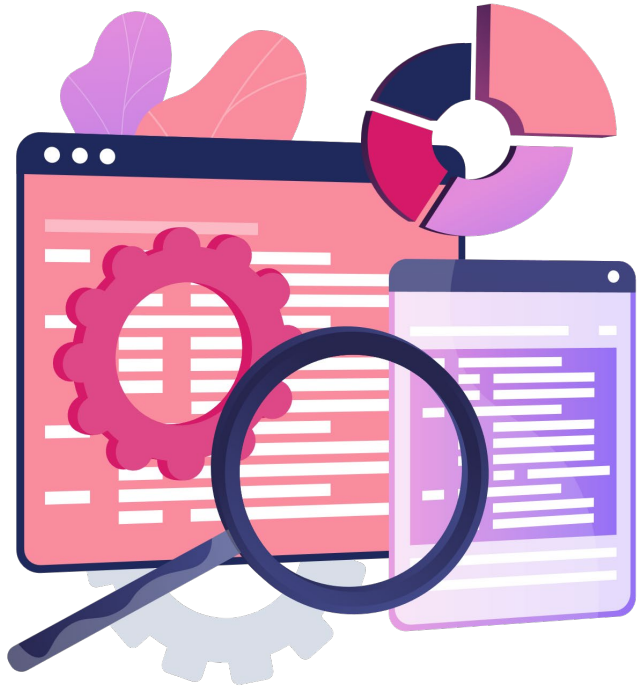
CHAPTER 9

SITE-TO-SITE VPN

YOU DESERVE THE BEST SECURITY

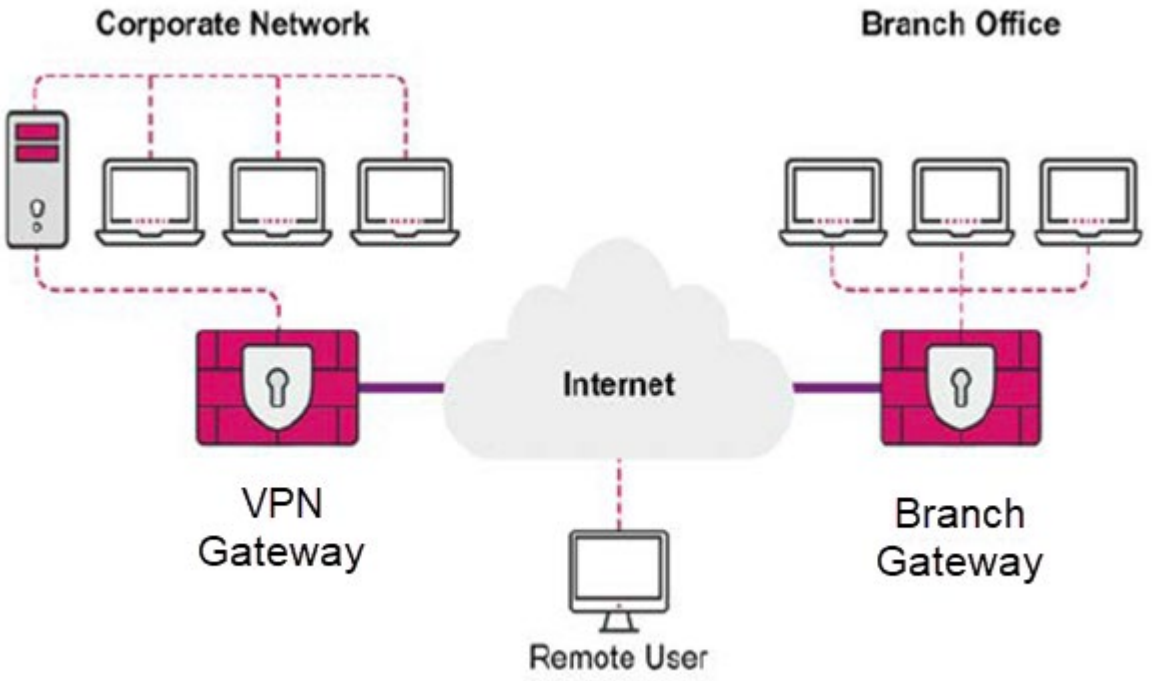
Learning Objectives

- Discuss Site-to-Site VPN basics, deployment, and communities.
- Describe how to analyze and interpret VPN tunnel traffic.
- Articulate how pre-shared keys and certificates can be configured to authenticate with third-party and externally managed VPN Gateways.
- Explain Link Selection and ISP Redundancy options.
- Explain tunnel management features.



Introduction to VPN

- A VPN securely connects networks and protects the data that passes between them.
- Tunnels are used to securely encrypt and decrypt the network communications.
- A VPN Gateway provides virtual connectivity and security for a wide range of situations.



The IPSec VPN Solution

- Lets the Security Gateway encrypt and decrypt traffic to and from other Security Gateways and clients.
- SmartConsole is used to easily configure VPN connections between Security Gateways and remote devices.
- The VPN tunnel guarantees:
  - Confidentiality - All VPN data is encrypted.
  - Integrity - Uses industry-standard integrity assurance methods.
  - Authenticity - Uses standard authentication methods.

Internet Key Exchange (IKE)

- Standard key management protocol that is used to create the VPN tunnels.
- Authenticate peers.
- Agree on keys and methods to be used for encryption.
- Produce a symmetric key on both sides to use for encryption and decryption of data.

IKE Versions

1

IKEv1 - The default version that is supported on most new and older systems.

2

IKEv2 - The newer version supporting IPv6 but currently Check Point Remote Access VPN clients do not support it.

IKE Phase I

- Agreement of encryption methods that are used to protect the IKE communication
- Diffie-Hellman key creation and exchange
- This is used to create a shared-secret between the peers for use as a source for generating encryption keys.
- Authentication between peers using a Pre-Shared Secret or Certificates, per the configuration.

IKEv1 Phase I - Main Mode and Aggressive Mode.

IKEv2 Phase I - 0ne mode and consists of two packets.

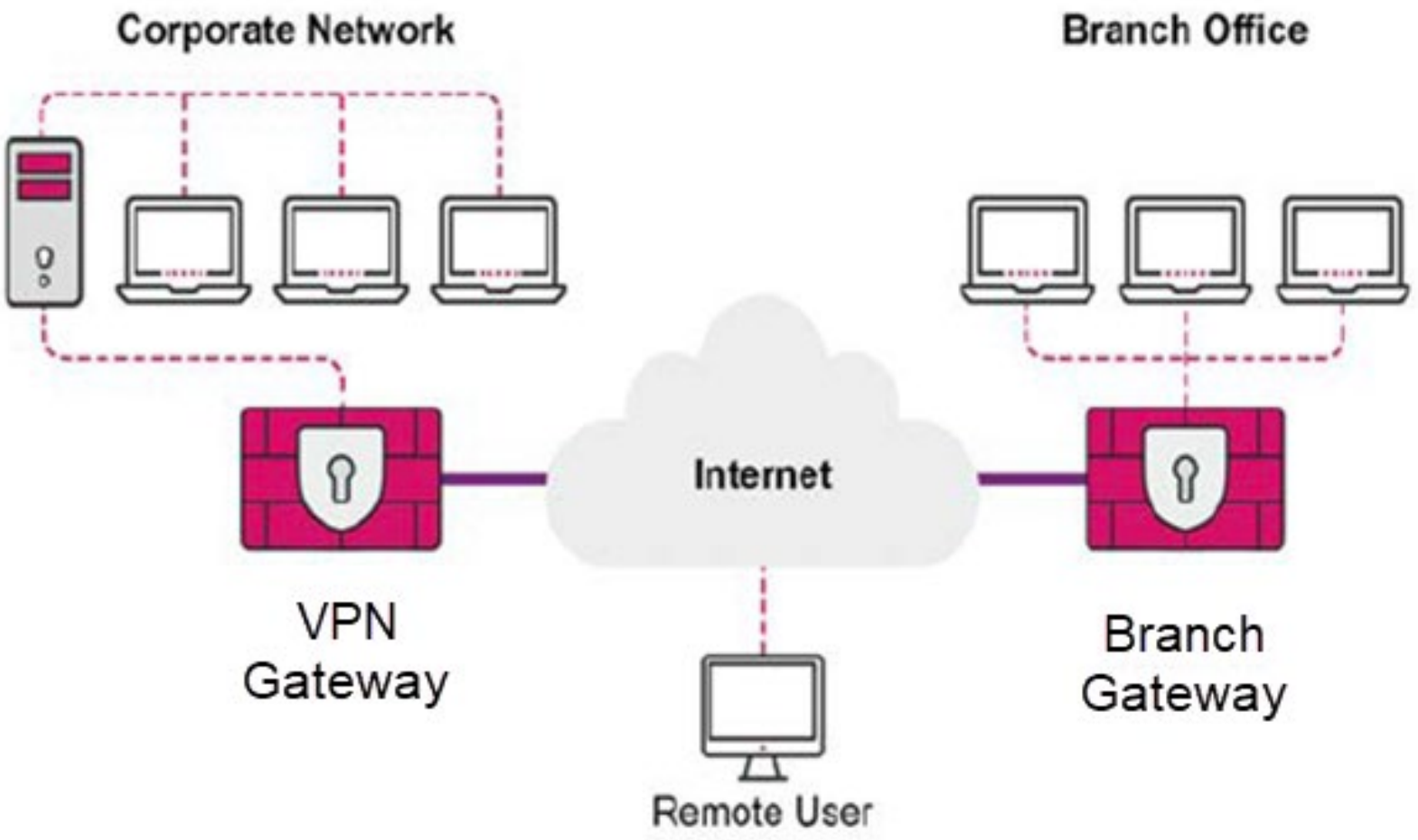
IKE Phase II

- Agreement of encryption methods that are used to protect the network traffic
- (Optional) Diffie-Hellman key exchange might happen based on the configuration of the Perfect Forward Secrecy (PFS) option
- Defining which networks or hosts need to secure the communication (VPN Domains)

IKEv1 Phase II - Quick Mode. Requires three packets for negotiation.

IKEv2 Phase II - Consists of two packets.

Site-to-Site VPN



IPSec VPN tunnels can be established between two Security Gateways to securely pass traffic between hosts behind these Security Gateways by encrypting and authenticating it.

Site-to-Site VPN (Continued)

Check Point Security Gateway

Check Point Security Gateway

- Managed by the same Management Server.

Check Point Security Gateway

- Managed by different Management Server.

Externally Managed VPN Gateway

Non-Check Point IPSec VPN

- Managed by a third-party.

Interoperable Device

Security Gateway Configuration

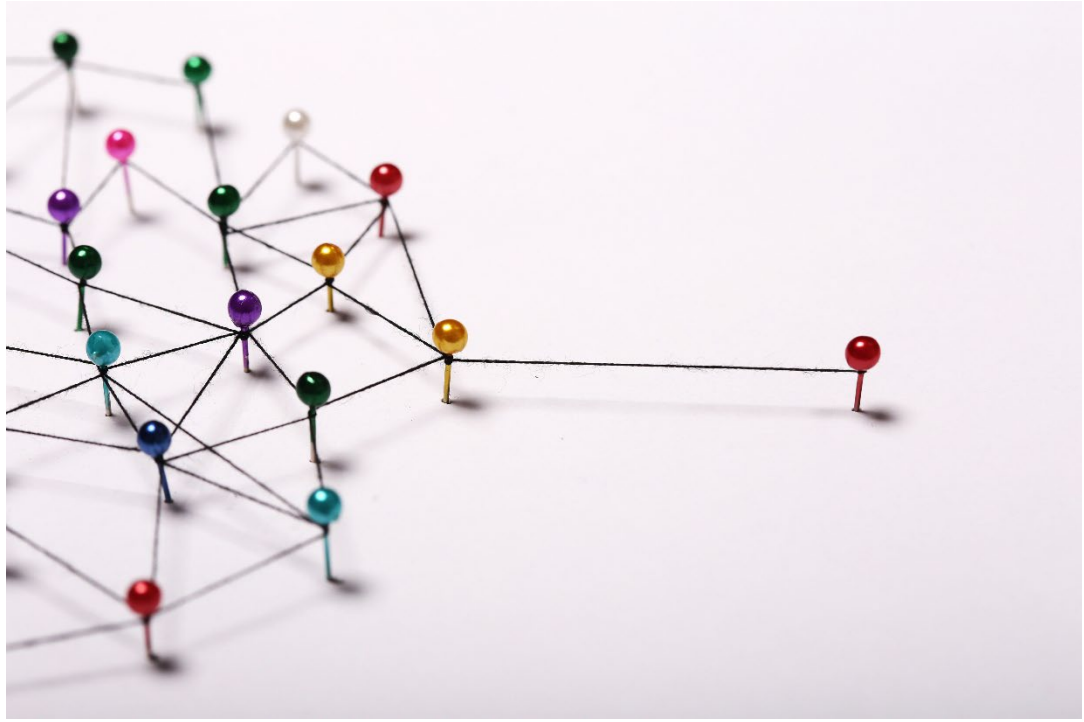
- Domain-based:
  - VPN domains are predefined for all VPN Gateways. A VPN domain is a host or network that can send or receive VPN traffic through a VPN Gateway.
- Route-based:
  - The Security Gateways have a Virtual Tunnel Interface (VTI) for each VPN Tunnel with a peer VPN Gateway.

Authentication Between Peer VPN Gateways

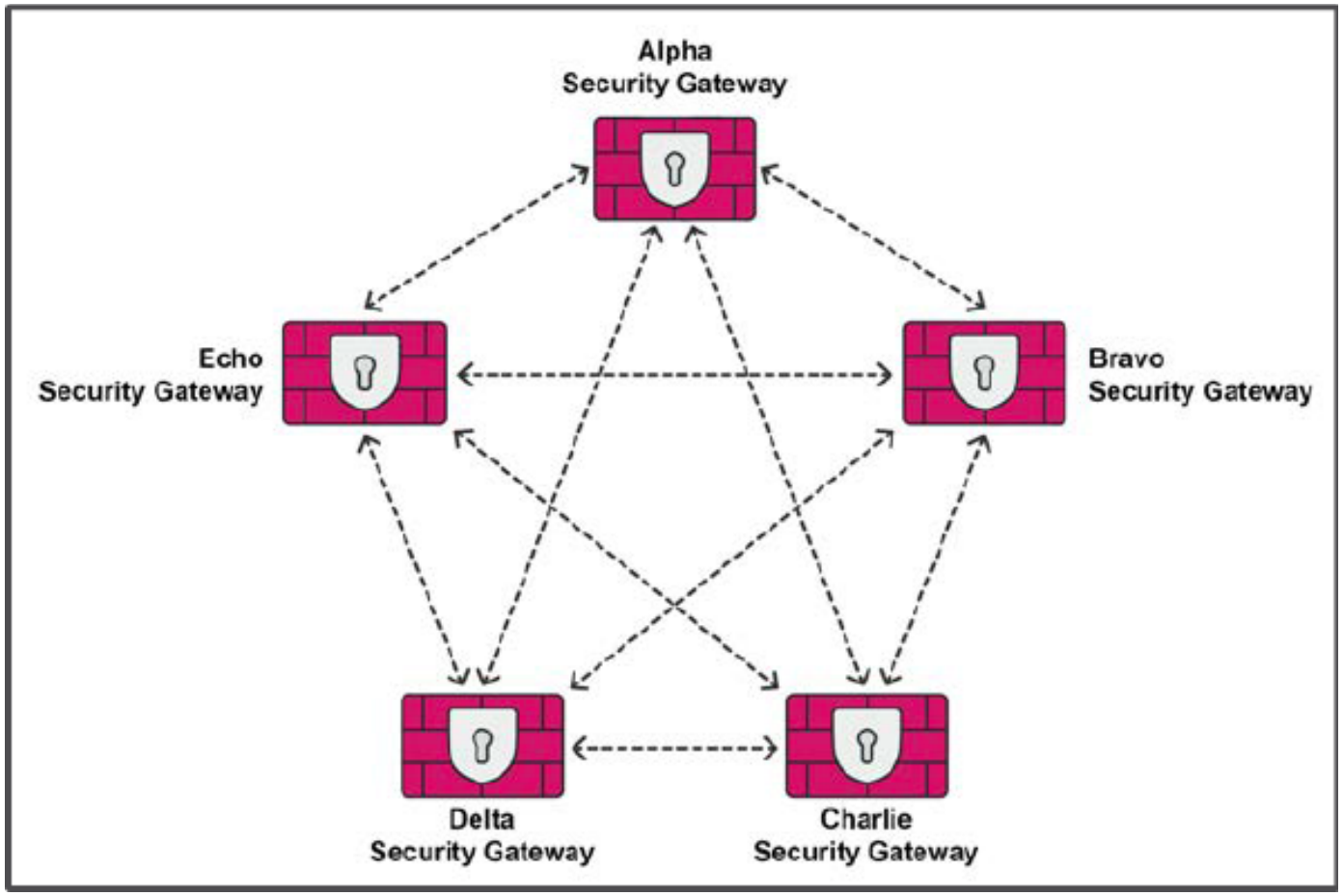
- IKE Phase I authentication based on one of the following:
  - Pre-shared secret
  - PKI certificate

VPN Communities

- Named collection of VPN domains (hosts/networks that use the Security Gateway to send/receive VPN traffic), each protected by a VPN Gateway.
- All attributes of the VPN Tunnels are defined in the VPN Community.
- Based on Mesh and Star topologies.

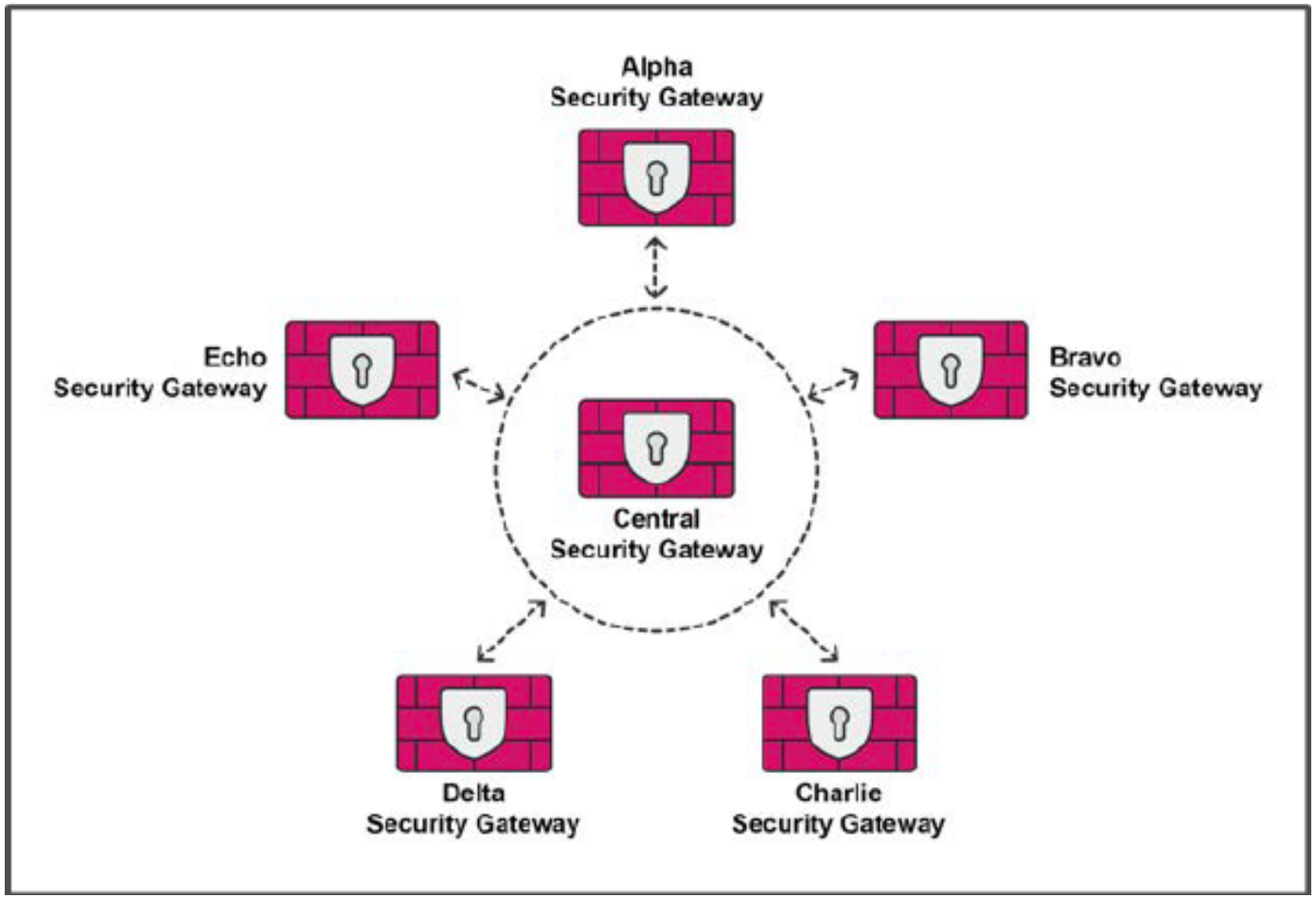


Mesh Topology



Any VPN Gateway in the Mesh community can establish a direct VPN tunnel with any peer Gateway in the Mesh community.

Star Community



One or more Center Gateways with Satellite Gateways as peers.

Combination of VPN Communities

- A VPN Gateway can be a member of more than one VPN Community if it does not pair with another VPN Gateway in more than one VPN Community.

Community 1 Mesh	Community 2 Star	Community 3 Mesh
• A-GW • B-GW • C-GW	Center: • A-GW	• A-GW • F-GW • G-GW
	Satellites: • D-GW • E-GW	

VPN Routing

- In a Star Community, two Satellite VPN Gateways cannot establish a VPN tunnel.
- If communication is required, traffic must be routed through the VPN tunnels the two Satellite VPN Gateways have with the Center VPN Gateway.
- Called VPN Routing because traffic is routed through two VPN tunnels.

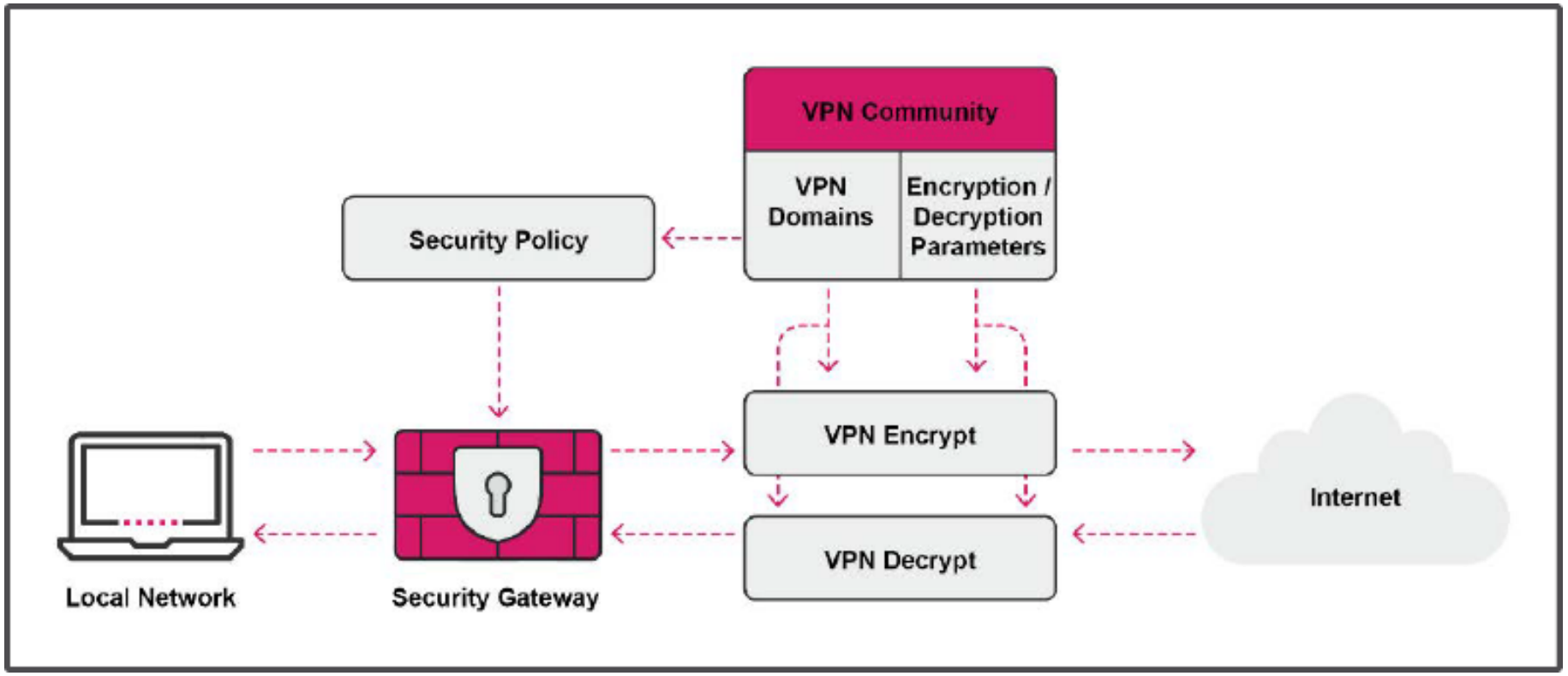
VPN Routing Options

The VPN Routing options available in Star VPN communities are from one Satellite to:

- To Center only.
- To Center and to other Satellites through Center.
- To Center, or through the Center to other Satellites, to Internet and other VPN targets.

Access Control for VPN Traffic

- Role of the Firewall is to allow or drop traffic, according to policy.



VPN Traffic Flow

- The traffic going out from the VPN Domain to the Internet hits the Firewall first.
- A decision is made whether to allow or drop the traffic.
- The rule that determines the action can based on the Source, Destination, and Service or it can include VPN Communities.

Even if the Source and Destination are left with Any, the rule is limited to the VPN Domains. The Source and Destination can be used to further limit the rule to certain hosts or direction.

Configuring Site-to-Site VPN - Considerations

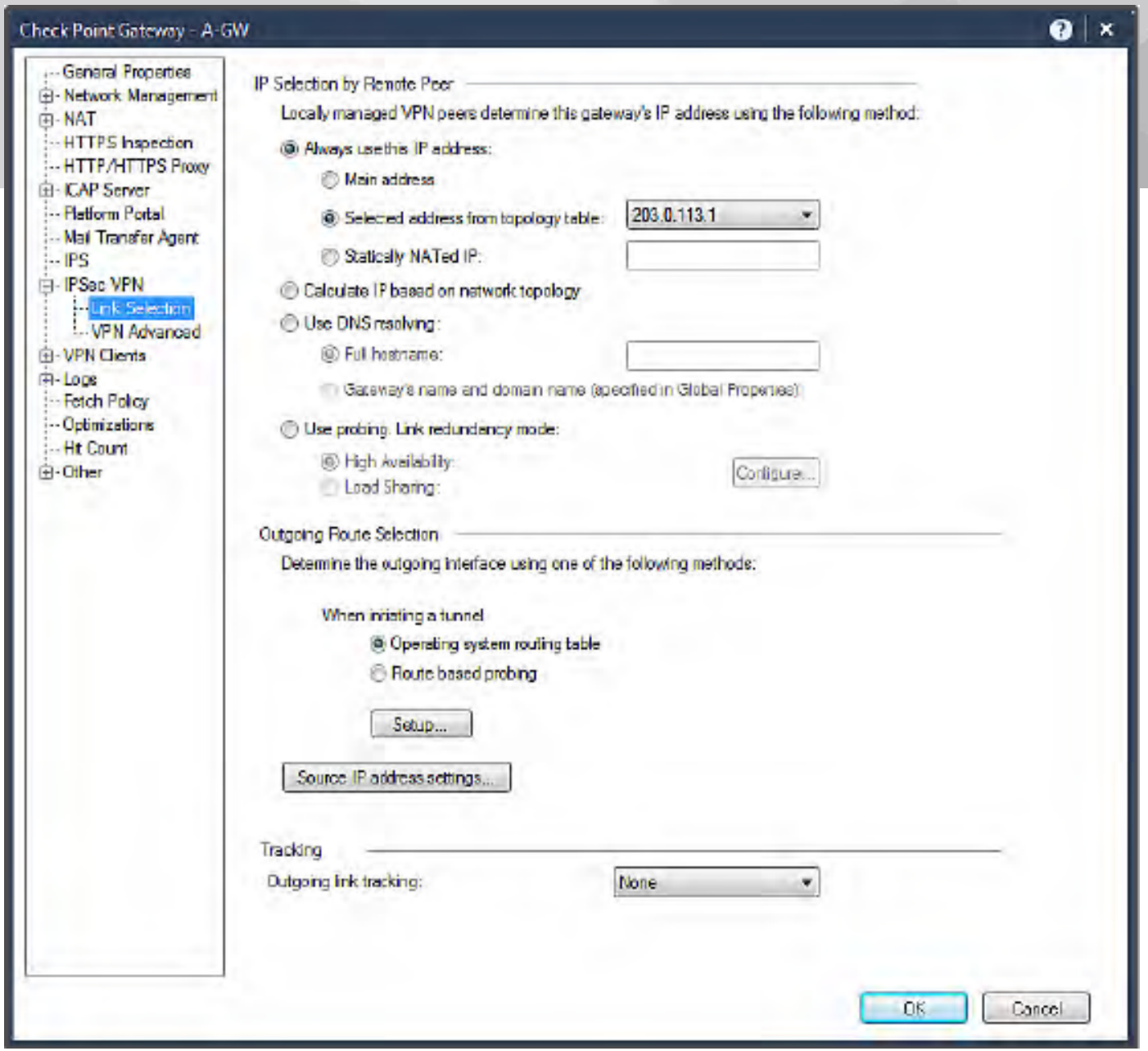
- What traffic from hosts/networks needs to be encrypted?
- Which Security Gateways perform the encryption and decryption?
- What encryption methods and IKE protocol will be used?
- What authentication method will be used?

Workflow

1. Enable IPSec VPN blade and set the VPN Domain (for Domain-based) & Link Selection for each Security Gateway object.
2. Create or use an existing default VPN community and add the Gateways.
3. Select the VPN Community encryption parameters, as needed.
4. Set the Tunnel Management and other Advanced properties.
5. For external or third-party VPNs, optionally select the Shared Secret.
6. Either add an explicit Firewall Rule to all traffic as required or enable the Encrypted Traffic option in the VPN community.

Step 1

Enable IPSec VPN Blade, set the VPN domain, and configure link selection.



Step 2

- Add Gateways to community.
  - Create a new VPN community or use an existing default VPN Community. Add the Gateways to the community.
  - The VPN community MyIntranet is a predefined Mesh Community. Administrators can use this default community or create a new VPN community by choosing a Mesh or Star topology.
  - In a Mesh community, the Participating Gateways list must include all VPN Gateways.

Step 3

- Select the VPN community encryption parameters, as needed.
- The encryption parameters apply to all the Gateways in the community; however, additional set of parameters can be defined for externally managed Gateways.

Parameter Name	Options
Encryption Method	IKEv1 / IKEv2
Encryption Algorithms	DES, 3DES, CAST, AES-128/256 & other variants
Hashing Algorithms	MD5, SHA1/256/384/512, AES-XCBC
Diffie-Hellman groups	Group 1/2/5/14/19/20

Step 4

- Tunnel management and other advanced properties.
  - Setting Permanent Tunnels
  - VPN Tunnel Sharing
- Tunnel Sharing options available in the community:
  - One VPN tunnel per each pair of hosts
  - One VPN tunnel per subnet pair
  - One VPN tunnel per Gateway pair

Step 5

For external or third-party VPNs, optionally select the Shared Secret.

If PKI certificates are not used, set a Shared Secret for each External VPN Gateway. This must match exactly what is set on the remote device and must be at least six characters; however, is recommended to have a secret of 20 or more characters

Step 6

- Create the VPN rules.
- To allow traffic between the VPN domains of internally managed VPN Gateways in a community, either:
  - Set Accept all encrypted traffic option.
  - Create an Explicit Firewall rule.

Review Questions

1. What is a VPN community?
2. Define IKEv1 and IKEv2.
3. List the two topologies on which VPN communities can be based.

Lab 9A

Configuring a Locally Managed Site-to-Site VPN