Using IPsec in the Enterprise

Joe Abraham
NETWORK SECURITY CONSULTANT
@joeabrah www.joeabrahamtech.com

Overview

Types of IPsec VPNs

IPsec implementation options

IPsec site-to-site VPN

IPsec remote access VPN

IPsec extras

Site-to-Site and Remote Acc

Added ‘Appear’ animations. If it worked for the content, you could also have each line left-to-right appear at a time to directly compare

Site-to-Site VPN

Logically connect sites together

GRE over IPsec (DMVPN)

Protects entire network

Provides corporate resources to other sites

Remote Access VPN

Logically connect endpoint to another network

IPsec using the OS IP stack

Protects individual devices

Provides individuals access to corporate resources

Useful in WiFi hotspots

IPsec Implementations

GRE with IPsec

GRE over IPsec

Encapsulate entire packet

DMVPN with IPsec

IPsec over GRE

Protect only the payload

Virtual Tunnel Interfaces

- Static or dynamic
- Site-to-site or remote access
- Can be quick IPsec setup
- Another basic option besides crypto maps

VRF Aware IPsec

Maps IPsec tunnels to MPLS VPNs to secure and encrypt traffic going out of the interfaces.

Remote Access VPN

Added animations to these icons and bullet text lines

Configured directly on OS or via application installed on device

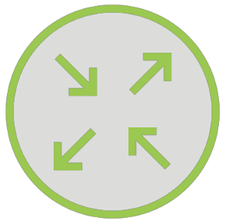
Many vendors and commercial services offer these types of VPNs

Used to access corporate resources or provide protection in public WiFi

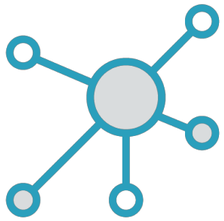
IPsec IPv4 to IPv6 Conversion

Dynamic Multipoint VPN

Added animations to these icons and bullet text lines



Next Hop Resolution Protocol (NHRP) helps route traffic over non-broadcast multiple access networks



Multipoint Generic Routing Encapsulation allows for a single interface to support many IPsec tunnels

IPsec is our IP security suite that protects our traffic!

Demo

Configure basic DMVPN with IPsec

- Only using AH, no ESP!

Verify IPsec operations

Analyze the traffic and debug the router

Demo

How we'll connect

Configure VPN through Windows machine

Analyze the traffic using Wireshark

Child SA

ISAKMP SA is the parent

- IPsec SA is created via the parent

  - Known as Child SA

NAT-Traversal

ESP does not have a port number

- How does PAT work for packets without dedicated port?

NAT-T detects NAT devices on path

ESP packets are encapsulated inside of UDP/4500 packets

Summary

Site-to-site versus remote access VPNs

IPsec implementations

DMVPN

Remote access

IPsec extras