IPSEC VPN TUNNEL

In Cisco Packet Tracer

Section Breaks

Introduction

The initial setup required and the terms used in this project will be explained

Implementation

The Actual code that drive the project is explained

Conclusion

Summary and overview

Introduction

01

What is VPN?

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

What is IPSec?

IPsec is a suite of related protocols for cryptographically securing communications at the IP Packet Layer. IPsec also provides methods for the manual and automatic negotiation of security associations (SAs) and key distribution, all the attributes for which are gathered in a domain of interpretation (DOI). The IPsec DOI is a document containing definitions for all the security parameters required for the successful negotiation of a VPN tunnel

A security association (SA) is a unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel.

ISAKMP

Uses well established protocols to exchange keys between 2 protocols

AES 256 Bit Encryption

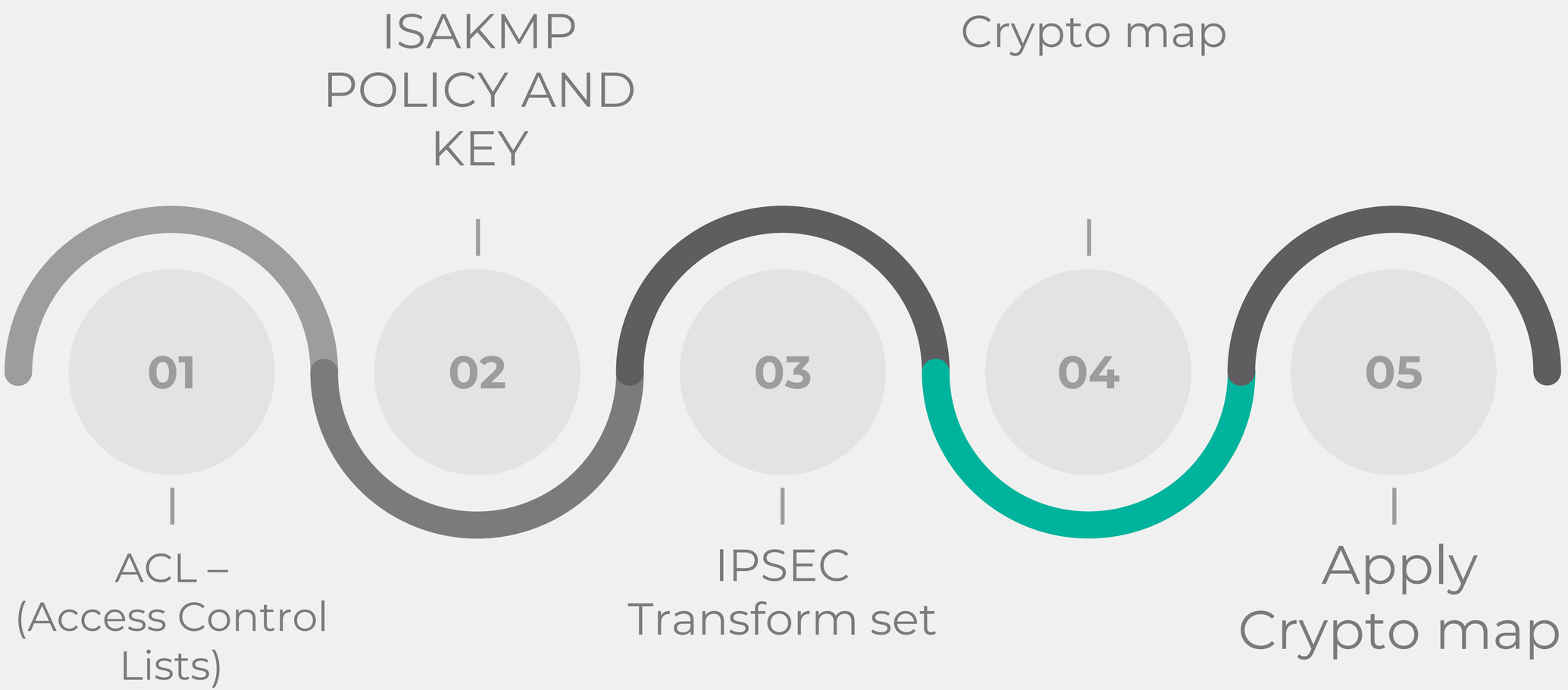
With 256 bit encryption data is transmitted very securely over the network

Diffie-Hellman Group 5

With 1536 bit key exchange the communication is highly secure

Implementation

02


ISAKMP POLICY AND KEY
Crypto map
01
02
03
04
05
ACL – (Access Control Lists)
IPSEC Transform set
Apply Crypto map

ACL :

(Permit Identical traffic to move in the tunnel)

ACLs are used to filter traffic based on the set of rules defined for the incoming or out going of the network.

access-list 100 permit ip *from-ip-add from-ip-wild card to-ip-add to-ip-wildcard*

ISAKMP Policy :

(Specifies the parameters to be used for exchange over the tunnel)

crypto ***name*** policy 10
encryption aes 256
authentication pre-share
group 5

ISAKMP KEY :

(It is a string of characters that is used as an authentication key)

Both gateways create a hash value based on the pre-shared key and other information. The hash values are then exchanged and verified to authenticate the other party.

crypto isakmp key *password* address *peer-router-add*

ISAKMP Transform Set :

(A transform set is a combination of individual IPSec transforms designed to enact a specific security policy)

* Mechanism for payload authentication (the process or action of verifying the identity of a user or process.)—AH transform
* Mechanism for payload encryption—ESP transform

crypto ipsec transform-set ***name*** esp-aes 256 esp-sha-hmac

ISAKMP MAP :

(A crypto map is a software configuration entity that performs certain functions)

A crypto map is a software configuration entity that performs two primary functions:

- Selects data flows that need security processing.
- Defines the policy for these flows and the crypto peer to which that traffic needs to go.

crypto map IPSEC-MAP 10 ***ipsec-name***
set peer ***peer-adds***
set pfs ***deffie-hellman-group***
set security-association lifetime seconds 86400
set ***transform-set-name***
match address 100

ISAKMP Apply:

(Apply the map on both routers)

interface ***name***
 crypto map IPSEC-MAP

Conclusion

03

Thank you!

BY
Vishwa Raghavendra 1DS17CS123
SIDDHARTH KOUL 1DS17CS112
SIDDHARTH SINGHI 1DS17CS113
AISHWARYA GUPTHA 1DS17CS130