

# IPsec Virtual Private Network

Understanding and Deploying IKEv1, IKEv2, GRE, IPsec VTI, FlexVPN

Aung Naing Moe

CCIE#50505

# IPsec Virtual Private Network

**Understanding and Deploying IKEv1, IKEv2, GRE, IPsec VTI, FlexVPN**

**Aung Naing Moe, CCIE No. 50505**

**Copyright © 2020 AMS Training**

**First published September 2020**

**Published by:**

**AMS Training**

**All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.**

## စာရေးသူ၏အမှာစာ

သတ္တမမြောက်စာအုပ်ဖြစ်တဲ့ IPsec မှတ်စုကတော့ Certification point of view ကြေည့်မယ်ဆိုရင်လည်း CCNA, CCNP, CCIE အတန်းအားလုံးမှာ ပါဝင်နေပါတယ်။ လက်တွေ့ လုပ်ငန်းခွင်ဘက်ကြည့်ပြန်ရင်လည်း အသုံးပြုတွင်ကျယ်နေတဲ့ technology တစ်ခုဖြစ်ပါတယ်။ ဒါကြောင့် IPsec အကြောင်း လေ့လာခဲ့သမျက် ကျွန်တော်နားလည်သလို ပြန်လည်မျှဝေလိုက်ပါတယ်။

ရေးသားပုံအစီစဉ်အနေနဲ့ကတော့ သီအိရိကို အရင်ဆုံးနားလည်အောင် ရှင်းပြထားပါတယ်။ သီအိရိနားလည်သွားတဲ့အခါ လက်တွေ့ ဘယ်လို လုပ်ရတယ်ဆိုတာ အဆင့်ဆင့် လုပ်ပြထားပါတယ်။ ရည်ရွယ်ချက်ကတော့ စာတွေ့၊ လက်တွေ့ မျှမျှတတ် လေ့လာနိုင်အောင် ဖြစ်ပါတယ်။ ငါသိ ငါတတ် ရေးထားတာ မဟုတ်တဲ့အတွက် မူရင်းအတိုင်း လေ့လာလိုသူများအတွက် reference လုပ်ထားတဲ့ မူရင်းဆရာတွေနဲ့ resource တွေကို ဖော်ပြပေးလိုက်ပါတယ်။

1. Cisco Press IKEv2 IPsec Virtual Private Network
2. BRKSEC-1050
3. CCIE Professional Development Series Network Security Technologies and Solutions.
4. INE CCIE Security Video
5. INE CCIE Security Work Book
6. CCIE Security work book By Narbik Kocharians
7. Cisco Documents and Internet စသည်ဖြစ်ပါတယ်။

ဒီစာအုပ် ဖြစ်မြောက်ဖို့အတွက် အဘက်ဘက်မှ ပိုင်းဝန်းကူညီပုံး စောက်ရှောက်ခဲ့ကြတဲ့ အနေ့ဌာ အနှစ် ငါးပါး အစထား၍ မိဘများနှင့် ဆရာများ အားလုံးကို ဒီနေရာကနေ ဂါရဝါပြု ကန်တော့ရပါတယ်။

လိုအပ်တဲ့အကြံ့ဗြာ်များ ပေးခဲ့တဲ့ ကိုသော်ငော်ဖြူး၊ အစစအရာရာ ကူညီစောင့်ရှောက် အကြံ့ပေးတဲ့အပြင် မအားလပ်တဲ့ကြားက စာအုပ်ကို စိစစ်ပေးပြီး၊ အမှာစာ ရေးသား

---

ချီးမြင်ပေးကြတဲ့ ဆရာ ကိုရဲနောင်း။ CCIE#44325 (Security)၊ ကိုဖြိုး (CCIE#38100, CISSP 570095) အထူး ကျေးဇူးတင် ဂါရိဝါယာပြုပါတယ်။

လိုလေသေးမရှိအောင် ကူညီပံ့ပိုးပေးတဲ့ ချစ်နှီး ဒေါက်တာစန်းသီတာဝင်း၊ သား မြတ်မိုးအေး သမီး သော်တာမိုးစံ တို့ကတော့ အထူး ကျေးဇူးတင်ရမယ့် သူတွေ ဖြစ်ပါတယ်။

ဒီစာအုပ်ကို ဖတ်ရှု၍ တစ်တရာ အကျိုးများခဲ့သည်ရှိသော် မူရင်းဆရာများကိုသာ ကျေးဇူးတင် မေတ္တာပို့သပေးဖို့ပဲဖြစ်ပါတယ်။ အကယ်၍အမှားယွင်း တစ်တရာ တွေခဲ့သည်ရှိသော် မူရင်းဆရာများရဲ့ အမှားမဟုတ်ပဲ ကျွန်တော့အမှားသာ ဖြစ်ပါတယ်။ ကျွန်တော့အနေနဲ့ ဆရာ ဆရာတွေ ကိုယ်စား ကျွန်တော်နား လည်သလို မြန်မာလို ပြန်လည်မျှဝေခြင်းများသာ ဖြစ်ပါတယ်။

တိုးတက်၊ အောင်မြင်၊ ပျော်ရွှင်၊ ပြီမ်းချမ်းကြပါစေ။

အောင်နှင်းမူး (AMS Training)

CCIE#50505 (RS)



## ဆရာကိုအောင်ဖြိုးလွင်၏ အမှာစာ

Network Engineer တစ်ယောက်ဖြစ်လာပြီဆိုရင် တစ်နေ့မဟုတ် တစ်နှာ VPN ဆိုတာနဲ့ ပက်သက်လာရမှာ အသေအချာပဲ ဖြစ်ပါတယ်။ VPN ဟာ နှစ်ပေါင်းများစွာကတည်းက Dial-up Network နဲ့ အသုံးပြုခဲ့တဲ့ နည်းပညာတစ်ခုဖြစ်သလို၊ တစ်ကမ္ဘာလုံးမှာရှိတဲ့ အဖွဲ့အစည်းတွေဟာ VPN ကို အသုံးချပြီး ကမ္ဘာအနဲ့က သူတို့ရုံးတွေကို အင်တာနက်ပေါ်ကနေ ချိတ်ဆက်ပြီး လုံခြုံ စိတ်ချွော့နဲ့ နေ့စဉ် အသုံးပြုနေကြတာ ဖြစ်ပါတယ်။ ယခု Cloud ခေတ်ရောက်လာတဲ့ အခါမှာလည်း Cloud နဲ့ ဆက်သွယ်တဲ့အခါမှာ အလျင်အမြန် တည်ဆောက်လို့ရပြီး လုံခြုံတဲ့ဆက်သွယ်မှု တစ်ခုအဖြစ်နဲ့ အသုံးပြုနေကြဆဲ ဖြစ်ပါတယ်။

ဒီလို အသုံးဝင်တဲ့ နည်းပညာတစ်ခုကို နားလည်ဖို့အတွက် ပါဝင်တဲ့ Protocol တွေ လုံခြုံရေးအတွက် Packet တွေ ဘယ်လိုစီမံလုပ်ဆောင်ပုံတွေကို လေ့လာဖို့လို့အပ်ပါတယ်။ ဒါမှာသာ ဘယ်လို Network Infrastructure နဲ့ ကြံလာသည် ဖြစ်စေ လိုအပ်လာတဲ့အခြေအနေအပေါ်မှာ ဖြစ်စေ VPN တည်ဆောက်ဖို့အတွက် ကိုယ်တိုင် စဉ်းစားလုပ်ဆောင်နိုင်မှာ ဖြစ်ပါတယ်။ အခု ကိုအောင်နိုင်မိုးရဲ့ IPsec VPN စာအုပ်ဟာ အဲဒီလို လေ့လာနေသူတွေ လေ့လာနိုင်ဖို့အတွက် လက်တွေ့လုပ်ဆောင်ချက်တွေနဲ့ မတူညီတဲ့ Network ပုံစံ အမျိုးမျိုးပေါ်မှာ နမူနာတွေနဲ့ တကွ အသေးစိတ် အဆင့်ဆင့် ရှင်းပြပေးထားတာ တွေ့ရပါတယ်။ ဒါကြောင့် VPN အကြောင်း လေ့လာရာမှာ အခက်အခဲ ဖြစ်နေတဲ့ သူတွေအတွက် အထောက်အကူပြုစေမည့် စာအုပ်တစ်အုပ်ဖြစ်ပါတယ်။

ဒီစာအုပ်မှာပါတဲ့ အကြောင်းအရာတွေဟာ စာမေးပွဲဖြေဆိုမည့်သူများအတွက် သာမက လက်တွေ့လုပ်ငန်းခွင် အတွက်ပါ အသုံးဝင်ပါတယ်။ အခုလို အကျိုးရှိစေမည့် စာအုပ်မှာ အမှတ်တရအဖြစ် အမှာစာ ရေးခွင့်ရတဲ့ အတွက်လည်း ဝမ်းမြောက်ဝမ်းသာ ဖြစ်မိပါတယ်။ စာဖတ်သူများအနေဖြင့်လည်း ဒီစာအုပ်မှာ ပါဝင်တဲ့ လက်တွေ့လုပ်ဆောင်မှုတွေကို ကိုယ်တိုင် လေ့လာ လိုက်လုပ်ရင်းနဲ့ IPsec VPN နဲ့ပက်သက်ပြီး အခက်အခဲမရှိရှင်းလင်းစွာနဲ့ နားလည်သွားမည်လို့ ယူဆမိပါတယ်။

ကိုဖြိုး

CCIE#38100, CISSP-570095

ဤစာအုပ်သည် **Ko Chit Paing Dway** ဝယ်ယူထားသော စာအုပ်ဖြစ်ပါသည်။

ဝယ်ယူသူအမည် = **Ko Chit Paing Dway**

Email = [chit.paingdway@gmail.com](mailto:chit.paingdway@gmail.com)

## Contents

<b>စာရင်းသူ၏အမှာစာ</b>	<b>i</b>
<b>ဆရာကိုအောင်ဖြုံးလွင်၏ အမှာစာ</b>	<b>iv</b>
<b>IPsec (Internet Protocol Security)</b>	<b>1</b>
VPN Overview .....	1
What is IPsec?	1
IPsec Feature.....	2
Confidentiality	2
Integrity	2
Peer Authentication and Data Origin Authentication	3
Anti-replay	3
Traffic flow confidentiality	3
Access Control	3
Why use IPsec VPN?.....	4
How IPsec works? .....	4
IPsec Framework	4
How IPsec tunnel works? .....	5
ISAKMP and IKE	6
Tunnel Mode and Transport .....	8
Tunnel Mode	8
Transport Mode	9
IKE (Internet Key Exchange).....	10
IKE Phase 1 .....	11
Step 2: DH Key Exchange	12
Step 3: Authentication	12
Main Mode.....	13
Message 1	13
Message 2	15
Message 3	16

---

Message 4	17
Message 5	17
Message 6	18
Aggressive Mode.....	19
Message 1	20
Message 2	22
Message 3	24
IKE Phase 2 .....	24
Message 1	25
Message 2	26
Message 3	26
IPsec Protocols .....	26
ESP (Encapsulating Security Payload) Protocol	26
Authentication Header Protocol	27
AH and ESP	28
<b>LAB 1 Site-To-Site VPN with Static IP (IOS to IOS)</b>	<b>30</b>
Diagram.....	30
Task .....	30
Lab 1 Solution.....	31
IPsec Site to Site VPN Configuration .....	32
Verification.....	34
Lab 1 Explanation.....	36
IPsec VPN requirement.....	37
Step – 1 Configure ISAKMP (IKE) - (ISAKMP Phase 1) .....	37
Step – 2 Configure IPSec (ISAKMP Phase 2, ACLs, Crypto MAP).....	38
NAT and site to site VPN .....	40
<b>LAB 2 Site-To-Site VPN with Dynamic IP address (IOS to IOS)</b>	<b>43</b>
Diagram.....	43
Task .....	43
Lab 2 Solution.....	44

---

## IPsec VPN

---

Verification.....	45
IPsec Site to Site VPN Configuration .....	45
Verification.....	48
Lab 2 Explanation.....	49
<b>Lab 3 Site-To-Site VPN with NAT-T</b>	<b>51</b>
Diagram.....	51
Task .....	51
Solution .....	51
Verification.....	53
Explanation .....	54
<b>Lab 4 Site-To-Site VPN with Aggressive mode (IOS to IOS)</b>	<b>57</b>
Diagram.....	57
Task .....	57
Lab 4 Solution.....	58
Verification.....	58
IPsec Site to Site VPN Configuration .....	59
Verification.....	60
<b>LAB 5 Site-To-Site VPN on ASA 9.7 using IKEv1</b>	<b>63</b>
Diagram.....	63
Configuration Steps.....	63
Verification.....	66
Lab 6 Command Explanation .....	67
<b>Internet Kye Exchange Version 2 (IKEv2 IPsec)</b>	<b>71</b>
IKEv2 Overview .....	71
Comparing IKEv1 and IKEv2 .....	71
IKEv2 CLI Overview.....	76
Introducing Smart Defaults.....	76
IKEv2 Proposal	78
Configuring IKEv2 Proposal	79

---

---

IKEv2 Policy	84
Configuring IKEv2 Policy	84
Default IKEv2 Policy	85
IKEv2 Keyring.....	85
IKEv2 Profile .....	85
Configuring IKEv2 Profile	86
<b>Lab – 1 Site to Site VPN with IKEv2 (IOS to IOS)</b>	<b>88</b>
Diagram.....	88
Task .....	88
Solution .....	88
Verification.....	92
Explanation .....	93
IKEv2 Proposal.....	93
<b>Lab – 2 Site to Site VPN with IKE v2 with NAT-T (IOS to IOS)</b>	<b>97</b>
Diagram.....	97
Task .....	97
Solution .....	97
Verification.....	101
Explanation .....	102
<b>Lab – 3 Site to Site VPN with IKE v2 with Dynamic IP</b>	<b>103</b>
Diagram.....	103
Task .....	103
Solution .....	104
Step 1 – IKEv2 Proposal (optional).....	104
Step 2 – IKEv2 Policy (optional) .....	105
Step 3 – Crypto IKEv2 keyring (optional) .....	105
Step 4 – Crypto IKEv2 profile .....	105
Step 5 – Crypto ACL and IPsec Transform Set.....	105
Step 6 – Crypto map.....	106

---

---

Verification.....	107
<b>Lab – 4 Site to Site VPN using IKEv2 on ASA 9.7</b>	<b>109</b>
Diagram.....	109
Task .....	109
Configuration Steps on ASA .....	109
Solution .....	110
Verification.....	112
Useful show command .....	112
Explanation .....	113
Encryption Domain .....	113
Phase 1 Proposal.....	113
Phase 2 Proposal.....	114
Tunnel Group .....	114
Crypto Map .....	115
Configuring PAT on ASA .....	115
Configuring NAT exemption.....	116
<b>Generic Routing Encapsulation (GRE) and IPsec</b>	<b>118</b>
What is GRE?.....	118
GRE over IPsec .....	119
IPsec over GRE .....	119
GRE Summary.....	120
<b>Lab – 1 GRE over IPsec with Crypto Profiles (IKEv1)</b>	<b>121</b>
Diagram.....	121
Task .....	121
Solution .....	122
Basic Configuration .....	122
GRE configuration .....	123
IPsec Configuration .....	123
Routing.....	124

---

Verification.....	125
<b>Lab – 2 GRE over IPsec with Crypto Maps (IKEv1)</b>	<b>126</b>
Diagram.....	126
Task .....	126
Solution.....	127
Basic Configuration .....	127
GRE configuration .....	127
IPsec Configuration.....	128
Routing.....	129
Verification.....	130
<b>Lab – 3 GRE over IPsec with Crypto Profiles (IKEv2)</b>	<b>131</b>
Diagram.....	131
Task .....	131
Solution.....	131
Basic Configuration .....	131
GRE configuration .....	132
IKEv2 Configuration.....	132
Routing.....	134
Verification.....	134
<b>Lab – 4 GRE over IPsec with Crypto Maps (IKEv2)</b>	<b>136</b>
Diagram.....	136
Task .....	136
Solution .....	136
Basic Configuration .....	136
GRE configuration .....	137
IKEv2 Configuration.....	137
Routing.....	139
Verification.....	140
<b>IPsec VTI</b>	<b>142</b>

---

## IPsec VPN

---

SVTI Theory Brief.....	142
When do you use SVTI? .....	143
Advantages and Disadvantages of SVTI	143
Summary of VTI	144
<b>Lab – 1 IPsec Static Virtual Tunnel Interfaces (IKEv1)</b>	<b>145</b>
Diagram.....	145
Task .....	145
Solution .....	146
<b>Lab – 2 IPsec Static Virtual Tunnel Interface (IKEv2)</b>	<b>151</b>
Diagram.....	151
Task .....	151
Solution .....	151
R2 configuration.....	152
R3 configuration.....	155
Verification.....	156
Useful verification commands	157
<b>FlexVPN</b>	<b>158</b>
What is FlexVPN? .....	158
VPN Technology Selection .....	158
Benefits of FlexVPN.....	160
When do you use FlexVPN? .....	161
FlexVPN Building Blocks .....	161
Cisco IOS Point-to-Point Tunnel Interfaces.....	161
Configuring P2P interface	162
Configuring virtual-template interface	162
Cisco IOS AAA Infrastructure .....	164
Benefits of Per-Peer P2P Tunnel Interface .....	164
<b>Lab – 1 Flex VPN Site-to-Site with Crypto Map</b>	<b>165</b>
Diagram.....	165

---

---

Lab objective .....	165
Task .....	165
Solution .....	166
Step 1 – IKEv2 Proposal (optional).....	167
Step 2 – IKEv2 Policy (optional) .....	167
Step 3 – Crypto IKEv2 keyring (optional) .....	167
Step 4 – Crypto IKEv2 profile .....	168
Step 5 – Crypto ACL and IPsec Transform Set.....	168
Step 6 – Crypto map.....	168
Verification.....	170
Explanation .....	171
<b>Lab – 2 Flex VPN with Site-to-Site with VTI</b>	<b>173</b>
Diagram.....	173
Task .....	173
Solution .....	173
R2 configuration.....	174
R3 configuration.....	177
Verification.....	178
Useful verification commands .....	179
<b>Lab – 3 Flex VPN with Hub and Spoke with ACL</b>	<b>180</b>
Diagram.....	180
Lab objective .....	180
Configuration Block.....	180
Task .....	181
Solution .....	181
Hub	181
Spoke	182
Verification.....	186
Explanation .....	187

---

<b>Lab – 4 Flex VPN with Hub and Spoke with BGP</b>	<b>189</b>
Diagram.....	189
Lab objective .....	189
Configuration Block.....	189
Task .....	190
Solution .....	190
Hub	190
Spoke	192
BGP	196
Verification	197
EIGRP	200
Explanation .....	201
<b>Lab – 5 Flex VPN HA Dual Hub and Dual Cloud</b>	<b>204</b>
Diagram.....	204
Objective .....	204
Task .....	204
Solution .....	205
Hub1	205
Hub2	207
Spokes	208
BGP Routing .....	214
Verification	216
Failover Test.....	220
R2's E0/0 Fail	220
R2's E0/1 Fail	220
<b>Lab – 6 Flex VPN HA Dual Hub using flex client</b>	<b>221</b>
Diagram.....	221
Objective .....	221
Task .....	221

---

## IPsec VPN

---

Solution .....	222
Hub1	222
Hub2	223
Spokes	225
EIGRP Routing .....	227
Verification	227
Failover Test.....	229
R2's E0/0 Fail	229
R2's E0/1 Fail	229
Explanation .....	229
Powerful peer syntax	229
Re-activation on Primary Peer	230
<b>Lab – 7 Flex VPN with Hub and Spoke with Auto mode</b>	<b>231</b>
Diagram.....	231
Lab objective .....	231
Configuration Block.....	231
Task.....	232
Solution .....	232
Hub	232
Spoke	233
BGP	238
Verification	239
EIGRP	240
<b>IPsec VPN Troubleshooting</b>	<b>241</b>
§Ω° †└	244



## IPsec (Internet Protocol Security)

### VPN Overview

ဒီသင်ခန်းစာမျာတော့ IPsec control plane တွေဖြစ်တဲ့ ISAKMP နဲ့ IKE အကြောင်းရယ်၊ IPsec Data Plane တွေဖြစ်တဲ့ ESP နဲ့ AH Encapsulation အကြောင်းလေ့လာရမှာဖြစ်ပါတယ်။ ဒီအကြောင်းတွေမလေ့လာခင် VPN ဆိုတာ ဘာလဲဆိုတာ အရင်လေ့လာ ကြည့်ရအောင်။

VPN ဆိုတာကတော့ Public network ပေါ်ကနေဖြတ်ပြီး၊ တစ်နေရာစီမှာကဲ့နေတဲ့ private network အချင်းချင်း အဆက်သွယ်ရအောင် လုပ်ပေးတဲ့ technology လို့ အကြမ်းဖျင်းမှတ်သားနှင့်ပါတယ်။

ဥပမာ - Ethernet VLANs, QinQ, Frame Relay PVCs, ATM PVCs, VPLS စတာတွေဟာ Layer 2 VPN တွေဖြစ်ပါတယ်။

GRE, MPLS Layer 3 VPN, IPsec စတာတွေကတော့ Layer 3 VPN တွေဖြစ်ပါတယ်။ အဲဒီထဲက IPsec VPN အကြောင်းလေ့လာကြရမှာဖြစ်ပါတယ်။

### What is IPsec?

IPsec (Internet Protocol Security) ဆိုတာကတော့ network layer မှာ သွားလာနေတဲ့ IP traffic တွေအားလုံး secure ဖြစ်အောင် protect လုပ်ပေးမယ့် standard framework တစ်ခုဖြစ်ပါတယ်။ IETF က develop လုပ်ထားတဲ့ open standard framework တစ်ခုဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ IP protocol မှာ ကိုယ်ပိုင် security feature မရှိလို့ဖြစ်ပါတယ်။ ဒါကြောင့် IPsec က secure ဖြစ်အောင် အောက်မှာဖော်ပြထားတဲ့ feature တွေကို သုံးပြီး security ကောင်းအောင် လုပ်ပေးမှာဖြစ်ပါတယ်။ RFC နဲ့ပက်သက်လို့ အများကြီး ရှိပါတယ်။ အသေးစိတ်ကိုတော့ အောက်မှာဖော်ပြထားတဲ့ RFC တွေမှာ ဖတ်ကြည့်ပါ။

- [RFC 2408](#) - Internet Security Association and Key Management Protocol (ISAKMP)
- [RFC 2409](#) - The Internet Key Exchange (IKE)

## IKEv1

- [RFC 4302](#) - IP Authentication Header
- [RFC 4303](#) - IP Encapsulating Security Payload (ESP)
- [RFC 5996](#) - Internet Key Exchange Protocol Version 2(IKEv2)

## IPsec Feature

IPsec framework ပေးတဲ့ security service တွေကတော့ အောက်ပါအတိုင်းဖြစ်ပါတယ်။

- Peer authentication
- Data confidentiality
- Data integrity
- Data origin authentication
- Replay detection
- Access control
- Traffic flow confidentiality စားတွေဖြစ်ပါတယ်။

## Confidentiality

Confidentiality ဆိုတာကတော့ သိခိုင်ရှိတဲ့သူကလဲလို့ တွေ့ခြားသူ မသိအောင် လျှို့ဝှက်ထားရမယ့် အရာဖြစ်ပါတယ်။ IPsec အနေနဲ့ sender နဲ့ receiver ကလဲလို့ တွေ့ခြားသူမှ data တွေကို ဖတ်လို့မရအောင် encryption လုပ်ခြင်းအားဖြင့် confidentiality မကျိုးပျက်အောင် တာဝန်ယူပါလိမ့်မယ်။ transit path မှာ ဖတ်ခိုင်ရှိတဲ့သူကလဲလို့ ဘယ်သူမှ ဖတ်လို့မရအောင် တာဝန်ယူမှာဖြစ်ပါတယ်။

## Integrity

Integrity ဆိုတာကတော့ sender နဲ့ receiver ကြားမှာ data တွေအပိုအယူလုပ်စဉ်မှာ တွေ့ခြားသူတစ်ယောက်က ကြားကနေဖြတ်ပြီး မူလ original data ကို ပြုပြင်ပြောင်းလဲမှု လုပ်လို့မရအောင် IPsec က ကာကွယ်ပေးမှာဖြစ်ပါတယ်။ hash value ကို calculation လုပ်ပြီး sender နဲ့ receiver အနေနဲ့ packet တွေဟာ လမ်းချေတ်မှာ တစ်စုံတစ်ယောက်က ပြုပြင်ပြောင်းလဲမှု လုပ်လိုက်သလား၊ မူလအတိုင်း ရောက်လာသလား ဆိုတာ စစ်နိုင်ပါတယ်။

## Peer Authentication and Data Origin Authentication

Authentication ဆိုတာကတော့ sender နဲ့ receive တွေဟာ အချင်းချင်း တကယ့် အစစ် ဟုတ် မဟုတ် စစ်ကြတာဖြစ်ပါတယ်။ ဒါ packet တွေက ဘယ်သူဆီ ကရောက်လာတာလဲဆိုတာကို လည်း စစ်မှုဖြစ်ပါတယ်။ Data ဟာ origin ဟုတ် မဟုတ် သိမှုဖြစ်ပါတယ်။ Data origin authentication လိုချေပါတယ်။

## Anti-replay

Anti-replay ဆိုတာကတော့ packet တွေကို encryption နဲ့ authentication လုပ်ပြီးတာတောင် Attacker အနေနဲ့ packet တွေကို capture လုပ်ပြီး အလယ်ကနေ အပိုအယူလုပ်နိုင်ပါတယ်။ IPsec အနေနဲ့ sequence number ကိုသုံးပြီး duplicate packet တွေကိုသိနိုင်ပါတယ်။ duplicate packet မှန်းသိတာနဲ့ transmit မလုပ်တော့ပါဘူး။ ဒါကြောင့် IPsec က sequence number ကို သုံးပြီး anti-replay attack ကိုလည်း ကာကွယ်ပေးနိုင်ပါတယ်။ ဒါကြောင့် ဒါ မျှ ပေါ်ပါတယ်။

## Traffic flow confidentiality

Network traffic တွေကို monitoring လုပ်နေတဲ့သူတွေအနေနဲ့ IPsec tunnel ထဲက သွားနေတဲ့ traffic တွေကို monitor မလုပ်နိုင်ပါဘူး။ ဆိုလိုတဲ့သောကတော့ ဘယ်သူနဲ့ဘယ်သူ အဆက်သွယ်လုပ်နေကြလဲ? ဘာတွေ ပို့နေကြလဲ မသိနိုင်ပါဘူး။ exchange လုပ်ထားတဲ့ packet amount ကိုတော့ သိနိုင်ပါတယ်။ ဒါကို traffic analysis protection လိုလည်း ခေါ်ပါတယ်။

## Access Control

IPsec endpoint အနေနဲ့ သက်ဆိုင်ရာ network resource ကို access လုပ်တဲ့သူဟာ တကယ့် access လုပ်ခွင့်ရှိတဲ့သူဆိုတာ သေချာအောင် filtering လုပ်နိုင်ပါတယ်။ ဒါကိုတော့ access control လိုချေပါတယ်။

## Why use IPsec VPN?

ဘာကြောင့် IPsec VPN ကိုသုံးရလဲခိုရင်တော့ အကြောင်းတွေက အများကြီးရှိပါတယ်။ ISP ဆီကနေ MPLS VPN လိုမျိုး သီးသန့် service ဝယ်စရာမလိုခြင်းကလည်း အကြောင်းတစ်ခု ဖြစ်ပါတယ်။ peer အချင်းချင်း IPv4 or IPv6 reachability ရှိပို့လိုပါတယ်။ site to site VPN အတွက်ပဲဖြစ်ဖြစ်၊ remote access VPN အတွက်ပဲဖြစ်ဖြစ် IPsec ကိုသုံးနိုင်ပါတယ်။ အကောင်းဆုံးအချက်ကတော့ data တွေ secure ဖြစ်အောင် protection လုပ် ပေးနိုင်လို့ဖြစ်ပါတယ်။ encryption လုပ်ဖို့အတွက် symmetric cipher ကိုသုံးပါတယ်။ (cipher ဆိုတာ secret code တစ်ခုထဲမှာ ရေးထားတဲ့ message ကိုဆိုလိုတာ ဖြစ်ပါတယ်။ စိုက်ဟလို့ အသံထွက်ပါတယ်။ စိုက်ဟလို့ အသံမထွက်ပါဘူး) ဥပမာ 3DES, AES တို့ဖြစ်ပါတယ်။ authentication အတွက် hashing ကိုသုံးပါတယ်။ ဥပမာ MD5, SHA တို့ဖြစ်ပါတယ်။ များသောအားဖြင့် P2P tunnel တွေမှာ အသုံးများပါတယ်။ P2MP ဖြစ်တဲ့ GETVPN ကတော့ ခြင်းချက်ဖြစ်ပါတယ်။

## How IPsec works?

IPsec က Network Layer မှာ အလုပ်လုပ်ပါတယ်။ SSL က layer 7 protocol ဖြစ်ပါတယ်။ အဓိကရည်ရွယ်ချက်ကတော့ IPv4 or IPv6 packet တွေကို encryption လုပ်ဖို့ authenticate လုပ်ဖို့ဖြစ်ပါတယ်။

## IPsec Framework

IPsec အနေနဲ့ network layer မှာ သွားနေတဲ့ IP packet တွေ secure ဖြစ်ဖို့ Confidentiality, Integrity, Authentication, Anti-replay စတဲ့ feature တွေကို implement လုပ်ဖို့ IPsec က အသုံးပြုတဲ့ protocol တွေကို သိထားသင့်ပါတယ်။ Figure 0-1 ကိုလေ့လာကြည့်ပါ။



**Figure 0 – 1**

IPsec protocol suite မှာ အဓိကအားဖြင့် encryption နဲ့ authentication အတွက် ESP နဲ့ AH ဆိုပြီး နှစ်ပိုင်းပါဝင်ပါတယ်။

Encryption အတွက် **DES, 3DES, AES** စတာတွေကို သံဃလိုရပါတယ်။ Authentication အတွက် **MD5** နဲ့ **SHA** ကိုသုံးလိုရပါတယ်။

IPsec ကို အသုံးပြုတဲ့အခါမှာတော့ router, firewall, server စတာတွေပေါ်မှာ အသုံးပြုလိုရပါတယ်။

ဥပမာ-

- Router နှစ်လုံးကြား site to site VPN အတွက်ပဲဖြစ်ဖြစ်
  - Firewall နဲ့ windows တွေကြားမှာ Remote access VPN အတွက်ပဲဖြစ်ဖြစ်
  - Linux server တွေကြားမှာ telnet လိုမျိုး secure မဖြစ်တဲ့ protocol တွေကို secure ဖြစ်အောင် လုပ်ပေးဖို့ပဲဖြစ်ဖြစ် စတာတွေအတွက်သုံးလိုရပါတယ်။
- အသုံးပြုတဲ့ပုံစံပေါ်မှုတည်ပြီး Implementation လုပ်တဲ့ပုံစံကွဲဘွားပါလိမ့်မယ်။

### How IPsec tunnel works?

IP packet တွေကို protection လုပ်ဖို့အတွက် အရင်ဆုံး peer နှစ်ခုဟာ IPsec tunnel တစ်ခု တည်ဆောက်ဖို့လိုပါတယ်။

## IKEv1

IPsec tunnel တည်ဆောက်ဖို့အတွက် IKE (Internet Key Exchange) protocol ကို သုံးပါတယ်။

### ISAKMP and IKE

ဒီနေရာမှာ Internet Security Association and Key Management Protocol (ISAKMP) နဲ့ Internet Key Exchange (IKE) အကြောင်း နည်းနည်းရှင်းပြလိုပါတယ်။ ဒီ term နှစ်ခုကတော့ သဘောတရား အတူတူဖြစ်ပါတယ်။ ISAKMP ဆိုတာကတော့ framework တစ်ခုဖြစ်ပြီး peer နှစ်ဘက် negotiate လုပ်ရမယ့် authentication, keying စတေတွေကို ရည်ညွှန်းတာ ဖြစ်ပါတယ်။ IKE ဆိုတာကတော့ actual implementation ကိုရည်ညွှန်းတာဖြစ်ပါတယ်။

#### Key Note:

**ISAKMP** describes the framework for key management and defines the procedure and packet format necessary to establish, negotiate, modify, and delete security association (SA). ISAKMP offers the identification of the peers only. It does not offer a key exchange mechanism.

**IKE** defines a proper key exchange mechanism for creating and exchanging keys. IKE uses UDP port 500.

IKE Phase နှစ်ခုရှိပါတယ်။

- **IKE phase 1**
- **IKE phase 2 တို့ဖြစ်ပါတယ်။**

IKE phase 1 မှာတော့ peer နှစ်ခုသုံးမယ့် parameter တွေကို ညီးစွမ်းဖို့ဖြစ်ပါတယ်။ နှစ်ဘက်သုံးမယ့် authentication method, encryption method, hashing method စတဲ့ protocol တွေ ဟိုဘက်၊ ဒီဘက် တူမတူ စစ်ရပါတယ်။ ဒီ phase မှာတော့ ISAKMP (Internet Security Association and Key Management Protocol) session တစ်ခုတည်ဆောက်ဖို့ဖြစ်ပါတယ်။ ISAKMP tunnel လို့လည်းခေါ်ပါတယ်။ IKE phase 1 လို့လည်း ခေါ်ပါတယ်။

Peer နှစ်ခုသုံးမယ့် parameter တွေစားတာကိုတော့ SA (Security Association) လို့ခေါ်ပါတယ်။ Figure 0 – 2 ကိုလေ့လာကြည့်ပါ။

## IKEv1



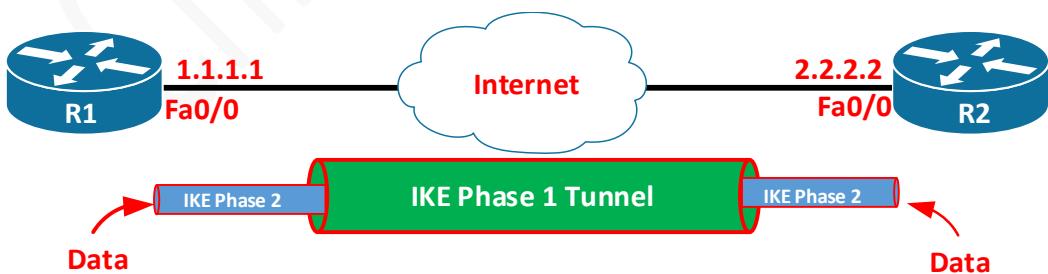
**Figure 0 – 2**

Traffic **တွက် management** လုပ်ဖို့အတွက် IKE Phase 1 tunnel ကိုသုံးပါတယ်။ IKE phase 2 tunnel secure ဖြစ်ဖို့ IKE phase 1 tunnel က အလွန်အင်မတန်မှ အရေးပါ ပါတယ်။ IKE phase 1 tunnel ထဲကနေ IKE phase 2 က သွားနေပုံဖြစ်ပါတယ်။ Figure 0 – 3 ကိုလေးလာကြည့်ပါ။



**Figure 0 – 3**

Data protection အတွက် IKE phase 2 tunnel ကိုသုံးပါတယ်။ user data traffic ဆုံး secure ဖြစ်ဖို့ IKE phase 2 က တာဝန်ယူတာဖြစ်ပါတယ်။ user data တွေက IKE phase 2 ထဲကနေ သွားနေပုံကို Figure 0-4 ကိုလေးလာကြည့်ပါ။



**Figure 0 – 4**

## IKEv1

IKE က tunnel တည်ဆောက်ပြီးတဲ့အခါ user data တွေကို authentication လုပ်ဖို့ encryption လုပ်ဖို့အတွက် အသံးပြုမယ့် protocol နှစ်ခုကိုလည်း သိဖို့လိုပါတယ်။ အဲဒီ protocol တွေကတော့ -

- **AH (Authentication Header)**
- **ESP (Encapsulating Security Payload)** တို့ဖြစ်ပါတယ်။

AH နဲ့ ESP နှစ်ခုစလုံးက authentication နဲ့ integrity ကို support လုပ်ပါတယ်။ ဒါပေမယ့် encryption ကိုတော့ ESP တစ်ခုတည်းကပဲ support လုပ်ပါတယ်။

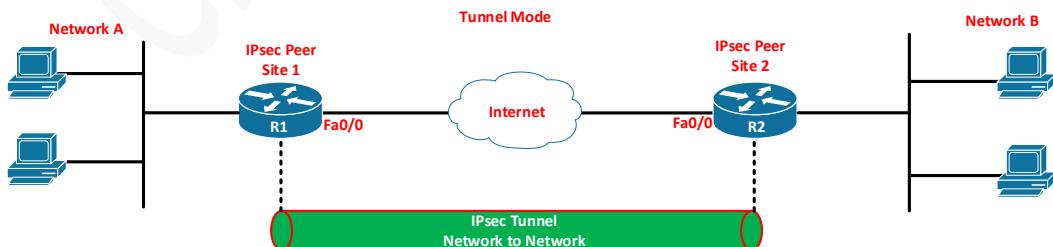
## Tunnel Mode and Transport

AH ရေး ESP ရေး နှစ်ခုစလုံးမှာ mode နှစ်ခုရှိပါတယ်။ အဲဒါတွေကတော့ -

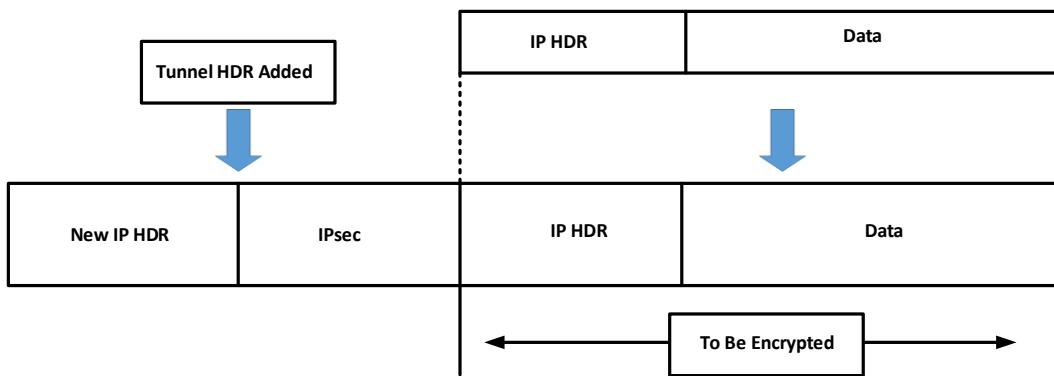
- Tunnel mode
- Transport mode တို့ဖြစ်ပါတယ်။

## Tunnel Mode

Network to network ဒါမူမဟုတ် site to site scenario တွေမှာ tunnel mode ကို သုံးလေ့ရှိပါတယ်။ ဥပမာ site1 မှာရှိတဲ့ network A နဲ့ site 2 မှာ ရှိတဲ့ network B ကိုချိတ်ဆက်တဲ့အခါမျိုး ဖြစ်ပါတယ်။ Tunnel mode က IP packet တစ်ခုလုံးကို encapsulate လုပ်ပြီး protect လုပ်ပေးပါတယ်။ payload, original IP header, new IP header အားလုံးပါဝင်ပါတယ်။ default က tunnel mode ဖြစ်ပါတယ်။ Figure 0-5 ကိုလေ့လာ ကြည့်ပါ။



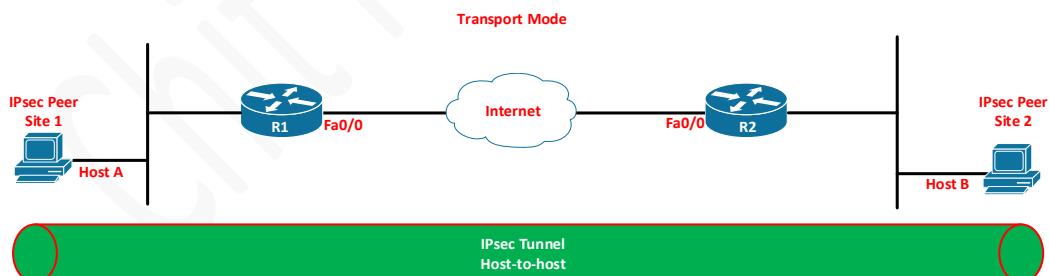
## IKEv1

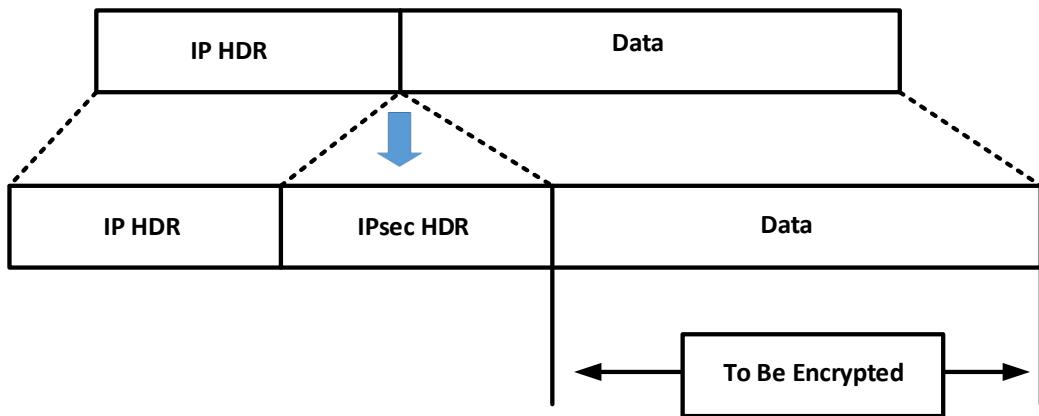


**Figure 0 – 5**

## Transport Mode

Host-to-host or end-to-end data protection scenario တွေမှာ အသုံးများပါတယ်။ ဥပမာ Site1 မှာရှိတဲ့ Host A နဲ့ Site2 မှာရှိတဲ့ Host B နဲ့ အဆက်သွယ်လုပ်တဲ့အခါမျိုးမှာဖြစ်ပါတယ်။ transport mode မှာ peer-to-peer scenario တွေမှာပဲ အသုံးပြုပါတယ်။ IPsec peer နှစ်ခုကြားမှာရှိတဲ့ traffic တွေကို encrypt လုပ်ပေးတာဖြစ်ပါတယ်။ transport mode မှာ IPsec အနေနဲ့ original IP datagram ရဲ့ payload ကိုပဲ protect လုပ်ပေးပါတယ်။ transport mode မှာ tunnel mode နဲ့ မတူတာကတော့ IPsec header ကို original IP header နဲ့ payload ကြားမှာ ထည့်လိုက်တာဖြစ်ပါတယ်။ figure 0 – 6 လေ့လာကြည့်ပါ။





**Figure 0 – 6**

Tunnel mode ကို pure IPsec တွေဖြစ်တဲ့ site to site VPN တွေမှာ အသုံးပြုလေ့ရှိပါတယ်။ Transport mode ကိုတော့ IPsec နဲ့ တိခိုး tunneling protocol တွေနဲ့ တွဲသုံးတဲ့ အခါမှာတွေမှာ အသုံးပြုလေ့ရှိပါတယ်။ ဥပမာ - GRE + IPsec လိုမျိုးဖြစ်ပါတယ်။

### **Key Point:**

**Transport mode:** Protects payload of the original IP datagram; typically used for end to-end sessions

**Tunnel mode:** Protects the entire IP datagram by encapsulating the entire IP datagram in a new IP datagram

### **IKE (Internet Key Exchange)**

IKE ကတော့ IPsec ရဲ့ အဓိကကျေတဲ့ protocol တစ်ခုဖြစ်ပါတယ်။ IKE version နှစ်ခုရှိပါတယ်။ အဲဒါတွေကတော့-

- IKEv1
- IKEv2 တို့ဖြစ်ပါတယ်။

IKEv1 ကို 1998 ဝန်းကျင်လောက်မှာ introduce လုပ်ခဲ့တာဖြစ်ပြီး၊ 2005 ခုနှစ်မှာတော့ IKEv2 ကို introduce လုပ်ခဲ့ပါတယ်။ IKEv1 ကို အရင်လေ့လာကြည့်ရအောင်။ IKEv2 လည်း နောက်လာမယ့်သင်ခန်းစာမှာ လေ့လာရမှာ ဖြစ်ပါတယ်။

## IKE Phase 1

IKE phase 1 ရဲအခိုကရည်ရွယ်ချက်ကတေသာ secure tunnel တစ်ခု တည်ဆောက်ဖို့  
ဖြစ်ပါတယ်။ IKE phase 1 အောင်မြင်ဖို့ peer နှစ်ခု ညီလိုင်းရမယ့် အဆင့်တွေကို step by step  
လေ့လာကြည့်ရအောင်။

### Step 1 Negotiation

Peer နှစ်ခုဟာ phase 1 အောင်မြင်ဖို့ ညီရမယ့်အချက်တွေကတေသာ အောက်ပါအတိုင်းဖြစ်ပါ  
တယ်။

**Hashing:** peer နှစ်ခုဟာ integrity ကို verify လုပ်ဖို့ hashing algorithm  
ကိုအသုံးပြုပါတယ်။ MD5 ဒါမှုမဟုတ် SHA ကိုသုံးပါတယ်။ နှစ်ဘက်စလုံး အသုံးပြုနေတဲ့  
hashing algorithm က တူဖို့လိုပါတယ်။ ဥပမာ MD5 ကိုသုံးရင် နှစ်ဘက်စလုံး MD5  
ဖြစ်ဖို့လိုပါတယ်။

**Authentication:** peer နှစ်ခုဟာ တစ်ယောက်ကိုတစ်ယောက် peer အစစ် ဟုတ် မဟုတ်  
စစ်ဖို့ လိုပါတယ်။ များသောအာဖြင့် pre-shared key နဲ့ digital certificate ကို  
သုံးလေ့ရှိပါတယ်။ နှစ်ဘက်တူဖို့လိုပါတယ်။

**DH (Diffie Hellman) group:** DH ဆိုတာကတေသာ crypto key exchange လုပ်ဖို့  
အသုံးပြုတဲ့ method ဖြစ်ပါတယ်။ DH group ပေါ်မှုတည်ပြီး key strength  
ဘယ်လောက်လဲဆိုတာ ကွဲသွားပါတယ်။ DH group number ကြီးလေ ပိုပြီး secure  
ဖြစ်တဲ့အတွက် ပိုကောင်းပါတယ်။ ဒါပေမယ့် CPU usage တော့ ပိုများသွားပါလိမ့်မယ်။  
ဘို့ဘက်ဒီဘက် တူဖို့လိုပါတယ်။

**Lifetime:** IKE phase 1 tunnel up နေတာ ဘယ်လောက်ကြောပြီလဲ? ဘယ်အချိန်မှာ ပြန်ပြီး  
negotiate လုပ်မလဲဆိုတာသတ်မှတ်ပေးဖို့ဖြစ်ပါတယ်။ default ကတေသာ 86400 seconds  
ဖြစ်ပါတယ်။ တစ်ရက်ပေါ့။

**Encryption:** encryption အတွက် ဘယ် algorithm ကိုသုံးမလဲ DES လား 3DES လား AES  
လား စသဖြင့် ဖြစ်ပါတယ်။ နှစ်ဦးနှစ်ဘက် တူဖို့လိုပါတယ်။

အချလေ့လာခဲ့တော့တွေကတော့ အဆင့်တစ် peer နှစ်ခု တစ်ယောက်နဲ့တစ်ယောက် အသုံးပြုမယ့် parameter တွေ တူ မတူ ညီးနှင့်နေတဲ့အဆင့်ဖြစ်ပါတယ်။

### **Step 2: DH Key Exchange**

Peer နှစ်ခုဟာ negotiation အောင်မြင်သွားတဲ့အခါ ဘယ် policy ကိုသုံးရမယ်ဆိုတာ သိသွားပါလိမ့်မယ်။ peer နှစ်ခုဟာ ပထမအဆင့်မှာ ညီးနှင့်ခဲ့တဲ့ keying Material ကို exchange လုပ်ဖို့ DH group ကိုသုံးမှာဖြစ်ပါတယ်။ အဲဒီလို exchange လုပ်ပြီးသွားတဲ့အခါ နှစ်ဦးနှစ်ဘက်လက်ခံထားတဲ့ shared key တစ်ခု ရသွားကြပါလိမ့်မယ်။

### **Step 3: Authentication**

နောက်ဆုံးအဆင့်အနေနဲ့ Peer နှစ်ခုဟာ အချင်းချင်း authentication လုပ်ကြပါလိမ့်မယ်။ အဲဒီလို authentication လုပ်တဲ့အခါမှာလည်း ရှေ့အဆင့်တွေမှာတူန်းက ညီးနှင့်စဉ်က နှစ်ဦးနှစ်ဘက် သဘောတူခဲ့တဲ့ authentication method ကိုသုံးမှာဖြစ်ပါတယ်။ authentication successful ဖြစ်သွားတယ်ဆိုရင်တော့ IKE phase 1 ဟာ complete ဖြစ်သွားပါပြီ။

အချလေ့လာခဲ့တဲ့ IKE phase 1 ကို configure လုပ်တဲ့အခါမှာ operation mode နှစ်ခုရှိပါတယ်။ အဲဒီတွေကတော့ -

- **Main mode**
- **Aggressive mode** တို့ဖြစ်ပါတယ်။

ဒီ Mode နှစ်ခုကတော့ tunnel တည်ဆောက်တဲ့အခါ အသုံးပြုတဲ့ message တွေပေါ်မှုတည်ပြီး ကဲ့သွားတာဖြစ်ပါတယ်။

Main mode ကိုသုံးပြီး tunnel တည်ဆောက်တဲ့အခါ message ခြောက်ခုကို အသုံးပြုပါတယ်။ ဆိုလိုတာက main mode model က six-way packet ကိုသုံးတာလို့ ပြောတာဖြစ်ပါတယ်။ aggressive mode ကတော့ message သုံးခုကို အသုံးပြုပါတယ်။ main mode က ပိုပြီး secure ဖြစ်ပါတယ်။ Cisco device တွေကတော့ Main mode ကို သုံးပါတယ်။ ဒါပေမယ့် တစ်ဘက် peer က aggressive ဖြစ်နေရင်လည်း respond လုပ်နိုင်ပါတယ်။

### Main Mode

IKE phase1 မှာ main mode က message ခြောက်ခုကို သုံးတယ်လို့ရှေ့မှာ ပြောခဲ့ပါတယ်။ အဲဒီ message ခြောက်ခုကို လေ့လာကြည့်ရအောင်။

### Message 1

Message တစ်ခုချင်းစီရင်းပြန့် Figure 0 – 7 ကိုသုံးပြီး ရှင်ပွဲပါမယ်။



**Figure 0 – 7**

Initiator ကနေ first message ကို စပိုပါတယ်။ Initiator ဆိုတာ tunnel တည်ဆောက်ဖို့ စပြီး ကြိုးစားတဲ့သူဖြစ်ပါတယ်။ Figure 0-8 ကိုလေ့လာကြည့်ပါ။ 197.0.0.2 က 196.0.0.2 ဆီကို စပြီး proposal message ပို့နေတာဖြစ်ပါတယ်။ IPsec က dialup connection လိုမျိုးပဲ packet စပို့မ tunnel up တာဖြစ်ပါတယ်။ 197.0.0.2 က initiator ဖြစ်ပြီး 196.0.0.2 က responder ဖြစ်ပါတယ်။ message 1 ထဲမှာ proposal ပါဝင်ပါတယ်။ proposal exchange လုပ်တာဖြစ်ပါတယ်။ အဲဒီ proposal ဆိုတာ DH group number တို့ encryption algorithm စတာတွေဖြစ်ပါတယ်။ အဲဒီ message ကို UDP packet ထဲမှာ ထည့်ပြီး သယ်သွားတာဖြစ်ပါတယ်။ **UDP port number 500 ကိုသုံးပါတယ်။** ပုံထဲမှာ Initiator SPI (Security Parameter Index) ကိုလေ့လာကြည့်ပါ။ အဲဒီမှာ unique value တစ်ခုပါဝင်ပါတယ်။ security association ကို identify လုပ်ဖိုဖြစ်ပါတယ်။

Figure 0 – 8 မှာ IKE version 1 နဲ့ main mode ဆိုတာ တွေ့ရမှာဖြစ်ပါတယ်။ domain of interpretation မှာ IPsec ဆိုတာတွေ့ရမှာဖြစ်ပါတယ်။ အဲဒီ ပထမဆုံး proposal ဖြစ်ပါတယ်။ transform payload မှာတော့ security association အတွက် သုံးမယ့် attribute တွေကို တွေ့ရမှာဖြစ်ပါတယ်။

## IKEv1

```

▷ Ethernet II, Src: c2:02:1a:dc:00:00 (c2:02:1a:dc:00:00), Dst:
▷ Internet Protocol Version 4, Src: 197.0.0.2, Dst: 196.0.0.2
▷ User Datagram Protocol, Src Port: 500, Dst Port: 500
└ Internet Security Association and Key Management Protocol
    Initiator SPI: bfe57d3e312fac07
    Responder SPI: 0000000000000000
    Next payload: Security Association (1)
    Version: 1.0
        Exchange type: Identity Protection (Main Mode) (2)
    Flags: 0x00
    Message ID: 0x00000000
    Length: 144
    Type Payload: Security Association (1)
        Next payload: Vendor ID (13)
        Payload length: 56
        Domain of interpretation: IPSEC (1)
    Situation: 00000001
    Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 44
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 1
    Type Payload: Transform (3) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 36
        Transform number: 1
        Transform ID: KEY_IKE (1)
    Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : AES-CBC
    Transform IKE Attribute Type (t=14,l=2) Key-Length : 128
    Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
    Transform IKE Attribute Type (t=4,l=2) Group-Description : 1536 bit MODP group
    Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
    Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
    Transform IKE Attribute Type (t=12,l=2) Life-Duration : 43200

```

**Figure 0 – 8**

**Message 2**

Responder အနေနဲ့ initiator ဆိုကနေ ပထမ message လက်ခံရရှိတဲ့အခါ အကြောင်းပြန် ရပါတယ်။ initiator ကပို့လိုက်တဲ့ transform payload ထဲမှာ ပါလာတဲ့ attribute တွေကို သဘောတူလက်ခံတဲ့အကြောင်း အကြောင်းကြားဖို့အတွက် message 2 ကို သုံးပါတယ်။ Figure 0-9 ကိုလေ့လာကြည့်ပါ။ responder မှာလည်း ကိုယ်ပိုင် SPI ရှိပါတယ်။

```

> Ethernet II, Src: c2:04:04:48:00:01 (c2:04:04:48:00:01), Dst: c
> Internet Protocol Version 4, Src: 196.0.0.2, Dst: 197.0.0.2
> User Datagram Protocol, Src Port: 500, Dst Port: 500
└ Internet Security Association and Key Management Protocol
    Initiator SPI: bfe57d3e312fac07
    Responder SPI: a1c5de50bdd407b9
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags: 0x00
    Message ID: 0x00000000
    Length: 104
    Type Payload: Security Association (1)
        Next payload: Vendor ID (13)
        Payload length: 56
        Domain of interpretation: IPSEC (1)
    Situation: 00000001
    Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 44
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 1
    Type Payload: Transform (3) # 1

```

## IKEv1

```

▲ Type Payload: Transform (3) # 1
  Next payload: NONE / No Next Payload (0)
  Payload length: 36
  Transform number: 1
  Transform ID: KEY_IKE (1)
    ▷ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : AES-CBC
    ▷ Transform IKE Attribute Type (t=14,l=2) Key-Length : 128
    ▷ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
    ▷ Transform IKE Attribute Type (t=4,l=2) Group-Description : 1536 bit MODP group
    ▷ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
    ▷ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
    ▷ Transform IKE Attribute Type (t=12,l=2) Life-Duration : 43200
  
```

**Figure 0 – 9**

## Message 3

Peer နှစ်ခုဟာ အချင်းချင်း အသုံးပြုမယ့် security association နဲ့ပက်သက်ပြီး သဘောတူညီမှု ရပြီတဲ့နောက် Diffie Hellman key exchange ကိစ္စ စလုပ်ပါတယ်။ အောက်က output ကို လေ့လာကြည့်တဲ့အခါ key exchange နဲ့ nonce အတွက် payload ကိုထွေ့ပါလိမ့်မယ်။

```

▷ Internet Protocol Version 4, Src: 197.0.0.2, Dst: 196.0.0.2
▷ User Datagram Protocol, Src Port: 500, Dst Port: 500
▲ Internet Security Association and Key Management Protocol
  Initiator SPI: bfe57d3e312fac07
  Responder SPI: a1c5de50bdd407b9
  Next payload: Key Exchange (4)
  ▷ Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ▷ Flags: 0x00
    Message ID: 0x00000000
    Length: 368
    ▷ Type Payload: Key Exchange (4)
      Next payload: Nonce (10)
      Payload length: 196
      Key Exchange Data: e567624cb8624cd08c90a2607ac83b75b893ba2cf3f8750...
    ▷ Type Payload: Nonce (10)
      Next payload: Vendor ID (13)
      Payload length: 24
      Nonce DATA: 1b6e0501f8ea56dc243b13074c999ddfc5a48a63
    ▷ Type Payload: Vendor ID (13) : CISCO-UNITY 1.0
      Next payload: Vendor ID (13)
      Payload length: 20
      Vendor ID: 12f5f28c457168a9702d9fe274cc0100
      Vendor ID: CISCO-UNITY
      CISCO-UNITY Major version: 1
      CISCO-UNITY Minor version: 0
  
```

**Figure 0 – 10**

## IKEv1

### Message 4

Responder ဖြစ်တဲ့ 196.0.0.2 ကလည်း initiator ဖြစ်တဲ့ 197.0.0.2 ကို Diffie Hellman nonce ကို ပိုလိုက်ပါတယ်။ အခုဆိုရင် peer နှစ်ခုဟာ Diffie Hellman shared key ကို calculation လုပ်လိုရပါပြီ။

```

> Internet Protocol Version 4, [Src: 196.0.0.2, Dst: 197.0.0.2]
> User Datagram Protocol, Src Port: 500, Dst Port: 500
└ Internet Security Association and Key Management Protocol
    Initiator SPI: bfe57d3e312fac07
    Responder SPI: a1c5de50bdd407b9
    Next payload: Key Exchange (4)
    ▶ Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    ▶ Flags: 0x00
    Message ID: 0x00000000
    Length: 368
    ▶ Type Payload: Key Exchange (4)
        Next payload: Nonce (10)
        Payload length: 196
        Key Exchange Data: 866d45c8fde7fe24dd52962fe7ff0fff6d585fcf82f56bfc...
    ▶ Type Payload: Nonce (10)
        Next payload: Vendor ID (13)
        Payload length: 24
        Nonce DATA: 836e9554c6a3efef4cb69258c54259f271d7f666
  
```

**Figure 0 – 11**

### Message 5

နောက်ဆုံး Message နှစ်ခုကတော့ encryption လုပ်ထားတဲ့အတွက် ကျွန်တော်တို့ စစ်လို့မရပါဘူး။ ဒါ message နှစ်ခုကတော့ identification နဲ့ authentication အတွက် သုံးတာဖြစ်ပါတယ်။ initiator ကင် စပိုတာဖြစ်ပါတယ်။ အောက်က output ကိုလေးလာကြည့်ပါ။

## IKEv1

```

> Frame 93: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
> Ethernet II, Src: c2:02:1a:dc:00:00 (c2:02:1a:dc:00:00), Dst: c2:04:04:48:00:01 (c2:04:04:48:00:01)
> Internet Protocol Version 4, Src: 197.0.0.2, Dst: 196.0.0.2
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
└ Internet Security Association and Key Management Protocol
    Initiator SPI: bfe57d3e312fac07
    Responder SPI: a1c5de50bdd407b9
    Next payload: Identification (5)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    └ Flags: 0x01
        Message ID: 0x00000000
        Length: 108
        Encrypted Data (80 bytes)

```

**Figure 0 – 12**

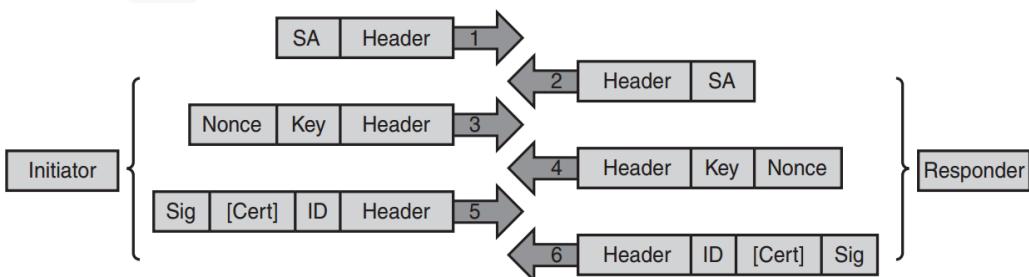
## Message 6

Responder ကလေး သူရဲ့ identification နဲ့ authentication ကို ပြန်ပြီး ပိုပေးပါတယ်။ အခုခံရင် IKEv1 main mode မှာ message ခြောက်ခွစလုံး ပြည့်စုံသွားပါပြီ။ IKE phase 2 ကိုဆက်ပြီး initiate လုပ်ပါလိမ့်မယ်။

```

> Frame 94: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
> Ethernet II, Src: c2:04:04:48:00:01 (c2:04:04:48:00:01), Dst: c2:02:1a:dc:00:00 (c2:02:1a:dc:00:00)
> Internet Protocol Version 4, Src: 196.0.0.2, Dst: 197.0.0.2
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
└ Internet Security Association and Key Management Protocol
    Initiator SPI: bfe57d3e312fac07
    Responder SPI: a1c5de50bdd407b9
    Next payload: Identification (5)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    └ Flags: 0x01
        Message ID: 0x00000000
        Length: 76
        Encrypted Data (48 bytes)

```

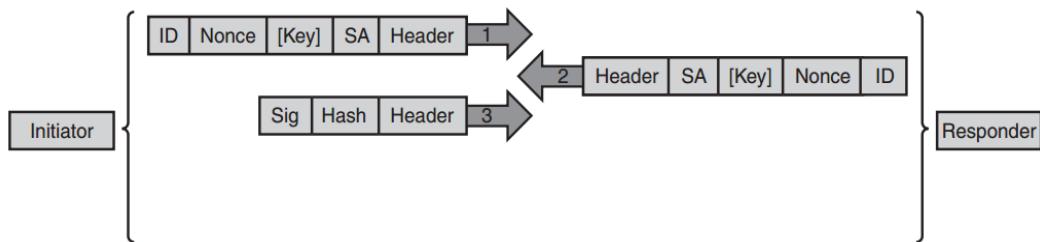


**Figure 0 – 13**

## IKEv1

### Aggressive Mode

IKEv1 Aggressive mode ကတေသ့ tunnel တစ်ခုတည်ဆောက်ဖို့ message သုံးခုပဲလိုပါတယ်။ main mode ထက်ပိုမြန်ပေမယ့် secure မဖြစ်ပါဘူး။ DH exchange လုပ်ဖို့လိုတဲ့ message အားလုံးကို ပထမ message နှစ်ခုထဲကို ထည့်လိုက်ပါတယ်။ Figure 0-14 ကိုလေ့လာကြည့်ပါ။



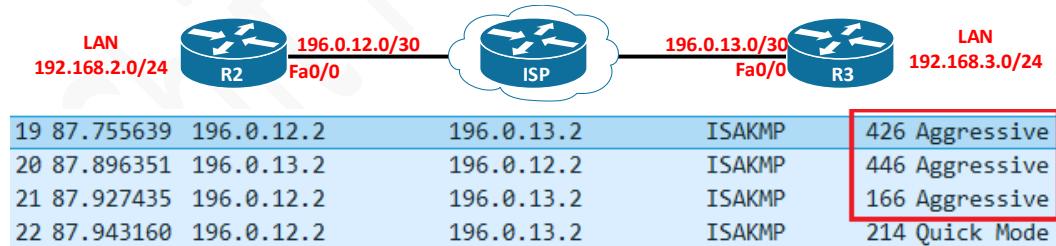
**Figure 0 – 14**

**MSG1:** Initiator key exchange, ID, nonce, parameter proposal

**MSG2:** Responder key exchange, ID, nonce, acceptable parameters

**MSG3:** Initiator signature, hash, ID

Wireshark နဲ့ capture လုပ်ပြထားတာတွေကို အဆင့်ဆင့်လေ့လာကြည့်ပါ။ R2 နဲ့ R3 ကို Aggressive mode ကိုသုံးပြု၍ site to site IPsec VPN configure လုပ်ထားပါတယ်။



## IKEv1

### Message 1

```

> Frame 19: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits) on interface 0
> Ethernet II, Src: c2:02:1f:30:00:00 (c2:02:1f:30:00:00), Dst: c2:01:0f:3c:00:00 (c2:01:0f:3c:00:00)
> Internet Protocol Version 4, Src: 196.0.12.2, Dst: 196.0.13.2
> User Datagram Protocol, Src Port: 500, Dst Port: 500
> Internet Security Association and Key Management Protocol
    Initiator SPI: 15a02535565379bd
    Responder SPI: 0000000000000000
        Next payload: Security Association (1)
        Version: 1.0
        Exchange type: Aggressive (4)
        Flags: 0x00
        Message ID: 0x00000000
        Length: 384
    > Type Payload: Security Association (1)
        Next payload: Vendor ID (13)
        Payload length: 56
        Domain of interpretation: IPSEC (1)
    > Situation: 00000001
    > Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 44
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 1
    > Type Payload: Transform (3) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 36
        Transform number: 1
        Transform ID: KEY_IKE (1)
        > Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC
        > Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
        > Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
        > Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
        > Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
        > Transform IKE Attribute Type (t=12,l=4) Life-Duration : 86400

```

## IKEv1

- ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07
- ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03
- ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
- Type Payload: Key Exchange (4)
  - Next payload: Nonce (10)
  - Payload length: 132
  - Key Exchange Data: ef3f69cb0034780e901865f5466bf160fefce03d44151287...
- Type Payload: Nonce (10)
  - Next payload: Identification (5)
  - Payload length: 24
  - Nonce DATA: f6f457f3d8fc7558806bca238be743551d5351fe
- Type Payload: Identification (5)
  - Next payload: Vendor ID (13)
  - Payload length: 12
  - ID type: IPV4\_ADDR (1)
  - Protocol ID: UDP (17)
  - Port: Unused
  - Identification Data: 196.0.13.2
  - ID\_IPV4\_ADDR: 196.0.13.2
- ▷ Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
- ▷ Type Payload: Vendor ID (13) : XAUTH
- ▷ Type Payload: Vendor ID (13) : CISCO-UNITY 1.0
- Type Payload: Vendor ID (13) : Unknown Vendor ID
  - Next payload: NONE / No Next Payload (0)
  - Payload length: 20
  - Vendor ID: e0678228565279bd98855427e6f6f8a0
  - Vendor ID: Unknown Vendor ID

First message မှာ initiator ဖြစ်တဲ့ 196.0.12.2 ကနေ responder ဖြစ်တဲ့ 196.0.13.2 ကို  
 message ပွဲနေတာဖြစ်ပါတယ်။ Message တစ်ခုထဲမှာပဲ transform payload များ security  
 association attributes, DH nonces နဲ့ identification (clear text) ဆောက်လောက်ပါတယ်။

## IKEv1

### Message 2

```

▷ Ethernet II, Src: c2:01:0f:3c:00:00 (c2:01:0f:3c:00:00), Dst: c2:02:1f:30:00:00 (c2:02:1f:30:00:00)
▷ Internet Protocol Version 4, Src: 196.0.13.2, Dst: 196.0.12.2
▷ User Datagram Protocol, Src Port: 500, Dst Port: 500
└ Internet Security Association and Key Management Protocol
    Initiator SPI: 15a02535565379bd
    Responder SPI: 54552762bbe9a906
    Next payload: Security Association (1)
    ▷ Version: 1.0
    Exchange type: Aggressive (4)
    ▷ Flags: 0x00
    Message ID: 0x00000000
    Length: 404
    ▷ Type Payload: Security Association (1)
        Next payload: Vendor ID (13)
        Payload length: 56
        Domain of interpretation: IPSEC (1)
        ▷ Situation: 00000001
    ▷ Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 44
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
    ▷ Type Payload: Transform (3) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 36
        Transform number: 1
        Transform ID: KEY_IKE (1)
        ▷ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC
        ▷ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
        ▷ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
        ▷ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
        ▷ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
        ▷ Transform IKE Attribute Type (t=12,l=4) Life-Duration : 86400

```

## IKEv1

- ▷ Type Payload: Vendor ID (13) : CISCO-UNITY 1.0
- ▷ Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
- ▷ Type Payload: Vendor ID (13) : Unknown Vendor ID
- ▷ Type Payload: Vendor ID (13) : XAUTH
- ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07
- Type Payload: Key Exchange (4)
  - Next payload: Identification (5)
  - Payload length: 132
  - Key Exchange Data: c1c450e12307d966817e6d0e7521a04cf... (truncated)
- Type Payload: Identification (5)
  - Next payload: Nonce (10)
  - Payload length: 12
  - ID type: IPV4\_ADDR (1)
  - Protocol ID: Unused
  - Port: Unused
  - Identification Data: 196.0.13.2
  - ID IPV4 ADDR: 196.0.13.2
- Type Payload: Nonce (10)
  - Next payload: Hash (8)
  - Payload length: 24
  - Nonce DATA: c86f7c18798f699b95ebb77a93301ea460f50c95
- Type Payload: Hash (8)
  - Next payload: NAT-Discovery (15)
  - Payload length: 20
  - Hash DATA: dc17cebcc2adfa065f8855ec77c1a01c
- ▷ Type Payload: NAT-Discovery (15)
- ▷ Type Payload: NAT-Discovery (15)

Message 2 မှာ responder အနေနဲ့ DH shared key တစ်ခု generate လုပ်ဖို့ လိုတဲ့  
 အချက်လက်အားလုံးပြည့်စုံနေပါ၍။ Initiator ဆိုကို nonce ပိုလိုက်ပါတယ်။ ဒါမှသာ initiator  
 အနေနဲ့ DH shared key ကို calculate လုပ်နိုင်မှာဖြစ်ပါတယ်။ authentication အတွက်  
 အသုံးပြုနေတဲ့ hash ကိုပါ calculate လုပ်မှာဖြစ်ပါတယ်။

## IKEv1

### Message 3

```

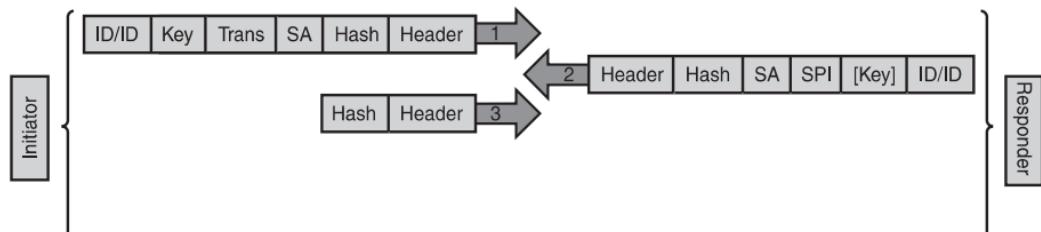
> Frame 21: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0
> Ethernet II, Src: c2:02:1f:30:00:00 (c2:02:1f:30:00:00), Dst: c2:01:0f:3c:00:00 (c2:01:0f:3c:00:00)
> Internet Protocol Version 4, Src: 196.0.12.2, Dst: 196.0.13.2
> User Datagram Protocol, Src Port: 500, Dst Port: 500
└ Internet Security Association and Key Management Protocol
    Initiator SPI: 15a02535565379bd
    Responder SPI: 54552762bbe9a906
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Aggressive (4)
    └ Flags: 0x01
        Message ID: 0x00000000
        Length: 124
        Encrypted Data (96 bytes)

```

နှစ်ဘက်စလုံးမှာ လိုတဲ့ အချက်လက်အားလုံးပြည့်စုံသွားပါပြီ။ IKE phase tunnel up သွားပါပြီ။ IKE phase 2 အတွက် ရွှေဆက်ပါလိမ့်မယ်။

### IKE Phase 2

IKE phase 2 tunnel (IPsec tunnel) ကတော့ user data ထွေကို protection လုပ်ပေးဖို့ သုံးတာဖြစ်ပါတယ်။ IKE phase 2 မှာတော့ phase 2 tunnel တည်ဆောက်ဖို့ mode တစ်ခုပဲ ရှိပါတယ်။ အဲဒါကတော့ quick mode ဖြစ်ပါတယ်။ figure 0-15 ကိုလေ့လာကြည့်ပါ။



**Figure 0 – 15**

**MSG1:** Hash, SA proposal, IPsec transform, keying material, ID

**MSG2:** Responder hash, agreed to SA proposal, Responder SPI, Key

**MSG3:** Hash to verify current and live peer

## IKEv1

IKE phase 1 လိုပဲ IKE phase 2 မှာလည်း peer တွေအချင်းချင်း negotiate လုပ်ရပါတယ်။ negotiate လုပ်ရမယ့်အချက်တွေကတော့ အောက်ပါအတိုင်းဖြစ်ပါတယ်။

**IPsec Protocol:** AH လား? ESP လား?

**Encapsulation Mode:** transport or tunnel mode?

**Encryption:** ဘယ် encryption method သုံးမလဲ? DES, 3DES or AES?

**Authentication:** authentication algorithm က ဘာသုံးမလဲ? MD5 or SHA?

**Lifetime:** IKE phase 2 tunnel က valid ဖြစ်သေးရဲ့လား? ဘယ်အချိန်မှာ expire ဖြစ်မလဲ?

**(Optional) DH exchange:** PFS (Perfect Forward Secrecy) ကိုသုံး၊ မသုံး

PFS ကတော့ optional ဖြစ်ပါတယ်။ IKE phase 2 quick mode မှာ new shared key generate လုပ်ဖို့အတွက် DH exchange ထပ် run ဖို့ peer တွေကို force လုပ်ဖို့ဖြစ်ပါတယ်။ အခါးလို့ Phase 2 negotiation က IKE phase 1 tunnel ထဲကနေ လုပ်နေတာဖြစ်တဲ့အတွက် IKE phase 1 က protection လုပ်ပေးထားပါတယ်။ ဒါကြောင့် ကျွန်တော်တို့အနေနဲ့ ဘာမှာတော့ မမြင်ရပါဘူး။

## Message 1

- ▷ Frame 95: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
- ▷ Ethernet II, Src: c2:02:1a:dc:00:00 (c2:02:1a:dc:00:00), Dst: c2:04:04:48:00:01 (c2:04:04:48:00:01)
- ▷ Internet Protocol Version 4, Src: 197.0.0.2, Dst: 196.0.0.2
- ▷ User Datagram Protocol, Src Port: 4500, Dst Port: 4500
- ▷ UDP Encapsulation of IPsec Packets
- ▲ Internet Security Association and Key Management Protocol
  - Initiator SPI: bfe57d3e312fac07
  - Responder SPI: a1c5de50bdd407b9
  - Next payload: Hash (8)
  - ▷ Version: 1.0
  - Exchange type: Quick Mode (32)
  - ▷ Flags: 0x01
  - Message ID: 0x519a3538
  - Length: 172
  - Encrypted Data (144 bytes)

## IKEv1

### Message 2

```

> Frame 96: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
> Ethernet II, Src: c2:04:04:48:00:01 (c2:04:04:48:00:01), Dst: c2:02:1a:dc:00:00 (c2:02:1a:dc:00:00)
> Internet Protocol Version 4, Src: 196.0.0.2, Dst: 197.0.0.2
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
└ Internet Security Association and Key Management Protocol
    Initiator SPI: bfe57d3e312fac07
    Responder SPI: a1c5de50bdd407b9
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
    Flags: 0x01
    Message ID: 0x519a3538
    Length: 172
    Encrypted Data (144 bytes)

```

### Message 3

```

> Frame 97: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: c2:02:1a:dc:00:00 (c2:02:1a:dc:00:00), Dst: c2:04:04:48:00:01 (c2:04:04:48:00:01)
> Internet Protocol Version 4, Src: 197.0.0.2, Dst: 196.0.0.2
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
└ Internet Security Association and Key Management Protocol
    Initiator SPI: bfe57d3e312fac07
    Responder SPI: a1c5de50bdd407b9
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
    Flags: 0x01
    Message ID: 0x519a3538
    Length: 60
    Encrypted Data (32 bytes)

```

IKE phase 2 complete ဖြစ်သွားပြီဆိုရင် user data တွေ tunnel ထဲကနေ လုလုခြုံမြှုနဲ့သွားလိုပါပြီ။

### IPsec Protocols

User data တွေကို protect လုပ်ဖို့ IPsec က သုံးနေတဲ့ protocol နှစ်ခုကတော့ AH နဲ့ ESP ဖြစ်ပါတယ်။ တစ်ခုစီခဲ့သုံးလို့ရသလို၊ နှစ်ခုစလုံးကို ပေါင်းပြီးတော့လည်း သုံးနိုင်ပါတယ်။

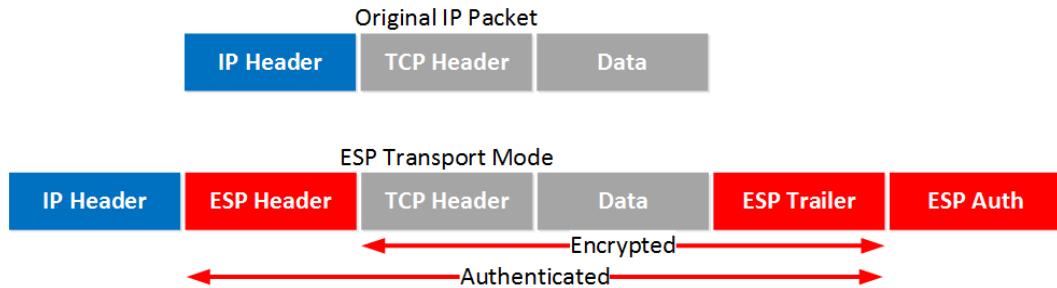
### ESP (Encapsulating Security Payload) Protocol

ESP ဆိုတာကတော့ IP-based protocol တစ်ခုဖြစ်ပါတယ်။ IPsec peer နှစ်ခု အချင်းချင်း အဆက်သွယ်လုပ်ဖို့အတွက် IP protocol number 50 ကိုသုံးပါတယ်။ ESP ကတော့ IP packet တွေကို encryption ပါ လုပ်ပေးနိုင်ပါတယ်။ transport mode ပဲဖြစ်ဖြစ်၊ tunnel mode

## IKEv1

ဖြစ်ဖြစ် သုံးလို့ရပါတယ်။ ESP ကို ဘာအတွက် သုံးလဲဆိုတော့ data confidentiality, data integrity, data authenticity အတွက် သုံးပါတယ်။ ESP က outer IP header ကိုတော့ protection မလုပ်ပေးပါဘူး။

### Transport mode



### Tunnel mode

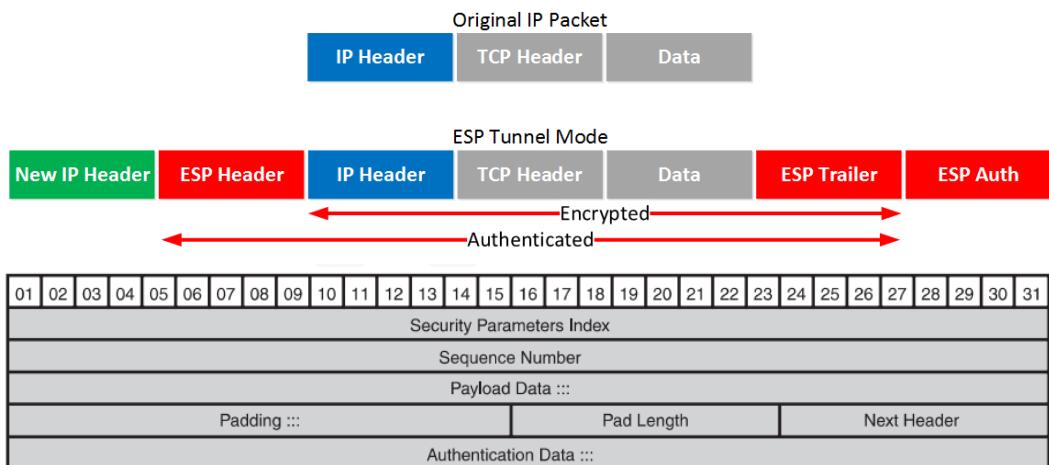


Figure 0 – 16 ESP Header Structure

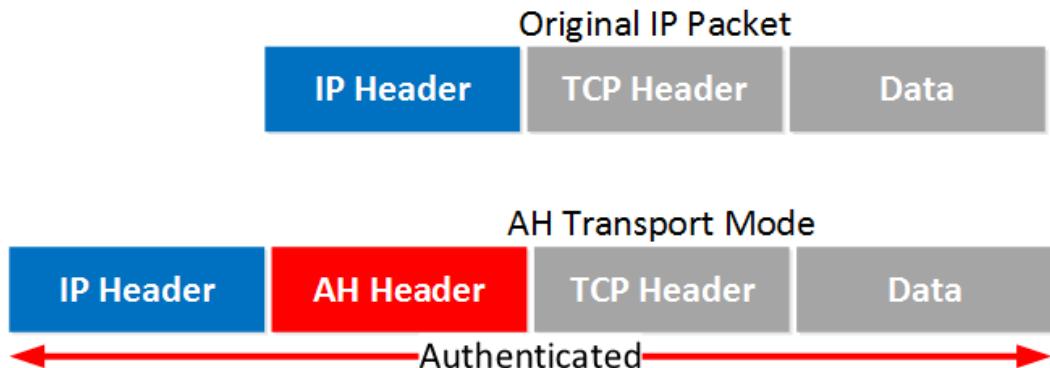
### Authentication Header Protocol

AH ဆိုတာကလည်း IP based protocol တစ်ခုဖြစ်ပါတယ်။ IPsec peer နှစ်ခု အချင်းချင်း အဆက်သွယ်လုပ်ဖို့အတွက် IP protocol number 51 ကို သုံးပါတယ်။ AH ကတော့ authentication နဲ့ integrity နှစ်ခုကို support လုပ်ပါတယ်။ encryption တော့ မလုပ်ပါဘူး။ hash value ကို calculation လုပ်ပြီး IP packet ကို protect လုပ်ပေးတာဖြစ်ပါ တယ်။

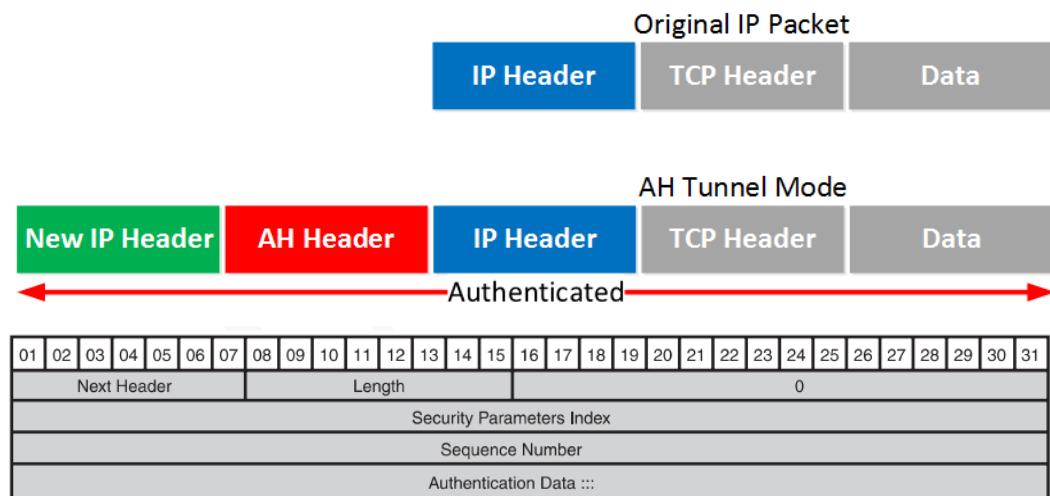
## IKEv1

### Transport mode

Transport mode မှာ IP header ထဲကို AH header ကို ထည့်လိုက်ပါတယ်။ အောက်မှာလေးလာကြည့်ပါ။



### Tunnel mode



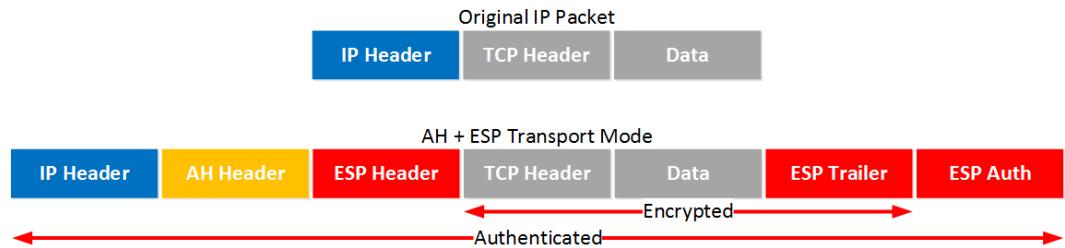
**Figure 0 – 17 AH Header Structure**

### AH and ESP

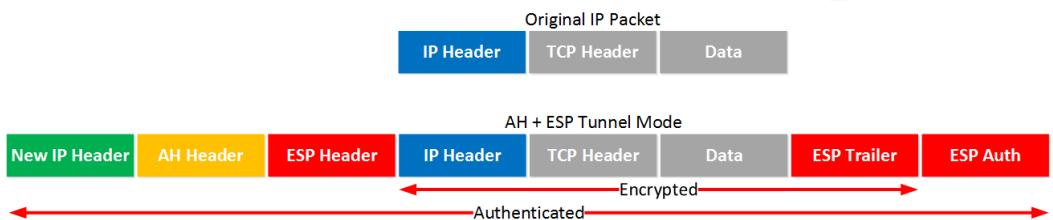
AH နဲ့ ESP ကတော့ အသုံးပြုပုံက confuse ဖြစ်တတ်ပါတယ်။ နှစ်ခုစလုံးကို တပြုင်နက်တည်းသုံးနိုင်ပါတယ်။

## IKEv1

### Transport mode

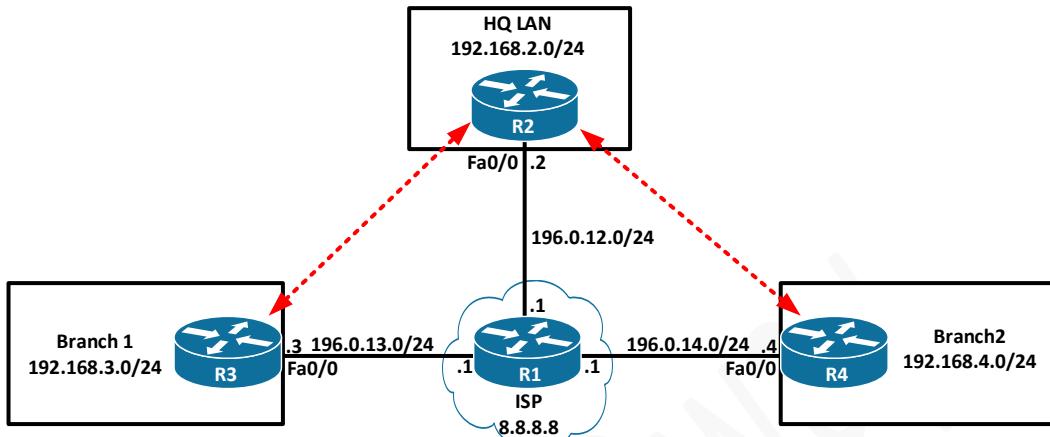


### Tunnel mode



## LAB 1 Site-To-Site VPN with Static IP (IOS to IOS)

### Diagram



### Task

- Configure site to site VPN between HQ and branch office 1 so that 192.168.2.0/24 and 192.168.3.0/24 communicate each other over the VPN tunnel. Ensure that all users can use internet as well.
- Configure site to site VPN between HQ and branch office 2 so that 192.168.2.0/24 and 192.168.4.0/24 communicate each other over the VPN tunnel. Ensure that all users can use internet as well.
- Use the following policy:

ISAKMP Policy	IPsec Policy
<b>Authentication: Pre-shared</b> <b>Encryption: 3DES</b> <b>Hash: MD5</b> <b>DH Group: 2</b> <b>PSK: AMS_KEY</b>	<b>Encryption: ESP-3DES</b> <b>Hash:MD5</b> <b>Crypto ACL:</b> <b>192.168.2.0/24 &lt;- -&gt; 192.168.3.0/24</b> <b>192.168.2.0/24 &lt;- -&gt; 192.168.4.0/24</b>

## Lab 1 Solution

**ISP**

```
R1(config)#hostname ISP
ISP(config)#int fa0/0
ISP(config-if)#description ISP_TO_R2
ISP(config-if)#ip add 196.0.12.1 255.255.255.0
ISP(config-if)#no shut
ISP(config-if)#int fa0/1
ISP(config-if)#no shut
ISP(config-if)#description ISP_TO_R3
ISP(config-if)#ip add 196.0.13.1 255.255.255.0
ISP(config-if)#int fa1/0
ISP(config-if)#no shut
ISP(config-if)#description ISP_TO_R4
ISP(config-if)#ip add 196.0.14.1 255.255.255.0
ISP(config-if)#exit
ISP(config)#int 10
ISP(config-if)#ip add 8.8.8.8 255.255.255.255
```

**R2 Basic Configuration**

```
R2(config)#int fa0/0
R2(config-if)#no shut
R2(config-if)#description R2_TO_ISP
R2(config-if)#ip add 196.0.12.2 255.255.255.0
R2(config-if)#int 10
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#ip route 0.0.0.0 0.0.0.0 196.0.12.1
```

**R3 Basic Configuration**

```
R3(config)#int fa0/0
R3(config-if)#no shut
R3(config-if)#description R3_TO_ISP
R3(config-if)#ip add 196.0.13.3 255.255.255.0
R3(config-if)#int 10
R3(config-if)#ip add 192.168.3.1 255.255.255.0
```

**R4 Basic Configuration**

```
R4(config)#int fa0/0
R4(config-if)#no shut
R4(config-if)#description R4_TO_ISP
R4(config-if)#ip add 196.0.14.4 255.255.255.0
R4(config-if)#int 10
R4(config-if)#ip add 192.168.4.1 255.255.255.0
R4(config-if)#ip route 0.0.0.0 0.0.0.0 196.0.14.1
```

## IKEv1

### Verification

```
R2#ping 196.0.13.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.0.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/115/128 ms
R2#ping 196.0.14.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.0.14.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/127/152 ms
R2#
```

## IPsec Site to Site VPN Configuration

**R2**

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# encr 3des
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# lifetime 43200
R2(config-isakmp)#exit
R2(config)#crypto isakmp key AMS_KEY address 0.0.0.0
0.0.0.0
R2(config)#ip access-list extended R2_TO_R3
R2(config-ext-nacl)# permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255

R2(config-ext-nacl)#ip access-list extended R2_TO_R4
R2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255
192.168.4.0 0.0.0.255

R2(config)#crypto ipsec transform-set AMS_SET esp-3des esp-
md5-hmac
R2(cfg-crypto-trans)#exit

R2(config)#crypto map AMS_VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
    and a valid access list have been configured.
R2(config-crypto-map)# set peer 196.0.13.3
R2(config-crypto-map)# set transform-set AMS_SET
R2(config-crypto-map)# match address R2_TO_R3
R2(config-crypto-map)#crypto map AMS_VPN 11 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
    and a valid access list have been configured.
```

## IKEv1

```
R2(config-crypto-map)# set peer 196.0.14.4
R2(config-crypto-map)# set transform-set AMS_SET
R2(config-crypto-map)# match address R2_TO_R4
R2(config-crypto-map)#exit
R2(config)#int fa0/0
R2(config-if)#crypto map AMS_VPN
R2(config-if)#
*Mar 1 00:39:24.603: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

### R3

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)# encr 3des
R3(config-isakmp)# hash md5
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# lifetime 86400
R3(config-isakmp)#crypto isakmp key AMS_KEY address
196.0.12.2
R3(config)#ip access-list extended R3_TO_R2
R3(config-ext-nacl)# permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
R3(config-ext-nacl)#crypto ipsec transform-set AMS_SET esp-3des
esp-md5-hmac
R3(cfg-crypto-trans)#crypto map AMS_VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R3(config-crypto-map)# set peer 196.0.12.2
R3(config-crypto-map)# set transform-set AMS_SET
R3(config-crypto-map)# match address R3_TO_R2
R3(config-crypto-map)#interface FastEthernet0/0
R3(config-if)# crypto map AMS_VPN
R3(config-if)#
*Mar 1 00:40:33.007: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

### R4

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)# encr 3des
R4(config-isakmp)# hash md5
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)# lifetime 86400
R4(config-isakmp)#crypto isakmp key AMS_KEY address
196.0.12.2
R4(config)#ip access-list extended R4_TO_R2
R4(config-ext-nacl)# permit ip 192.168.4.0 0.0.0.255
192.168.2.0 0.0.0.255
```

## IKEv1

```
R4(config-ext-nacl)#crypto ipsec transform-set AMS_SET esp-3des
esp-md5-hmac
R4(cfg-crypto-trans)#crypto map AMS_VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R4(config-crypto-map)# set peer 196.0.12.2
R4(config-crypto-map)# set transform-set AMS_SET
R4(config-crypto-map)# match address R4_TO_R2
R4(config-crypto-map)#interface FastEthernet0/0
R4(config-if)# crypto map AMS_VPN
*Mar 1 00:40:49.255: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R4(config-if)#

```

IPsec site to site VPN configuration လုပ်ပြီးသွားပါပြီ။ စစ်ကြည့်ပါမယ်။

```
R2#show crypto isakmp sa
dst                  src                  state            conn-id slot status
R2#show crypto ips sa
R2#show crypto session
R2#
```

ဘာ Tunnel မှ မတွေ့ရသေးပါဘူး။ ဘာကြောင့်လဲဆိုတော့ site to site vpn ရဲ့ သဘောက dialer connection လိုမျိုးပဲ traffic စပိုပြီး initiate လုပ်ကြည့်ရပါတယ်။ ဒါမှာ tunnel up မှာ ဖြစ်ပါတယ်။

## Verification

```
R3#ping 192.168.2.1 so 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 100/108/120 ms
R3#ping 192.168.2.1 so 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/140/156 ms
R3#
```

## IKEv1

```
R4#ping 192.168.2.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 100/103/112 ms
R4#ping 192.168.2.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
.!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/132/136 ms
R4#
```

Phase 1 စုစုပေါင်းမယ်။

```
R2#show crypto isakmp sa
dst          src          state      conn-id slot status
196.0.14.4   196.0.12.2  QM_IDLE    2        0 ACTIVE
196.0.13.3   196.0.12.2  QM_IDLE    1        0 ACTIVE
R2#
```

```
R2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
C-id Local          Remote          I-VRF      Status Encr Hash Auth DH Lifetime Cap.
2    196.0.12.2     196.0.14.4   ACTIVE 3des md5 psk 2  23:50:38
      Connection-id:Engine-id = 2:1(software)
1    196.0.12.2     196.0.13.3   ACTIVE 3des md5 psk 2  23:38:06
      Connection-id:Engine-id = 1:1(software)
R2#
```

```
R2#show crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 196.0.13.3 port 500
  IKE SA: local 196.0.12.2/500 remote 196.0.13.3/500 Active
  IPSEC FLOW: permit ip 192.168.2.0/255.255.255.0 192.168.3.0/255.255.255.0
              Active SAs: 2, origin: crypto map

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 196.0.14.4 port 500
  IKE SA: local 196.0.12.2/500 remote 196.0.14.4/500 Active
  IPSEC FLOW: permit ip 192.168.2.0/255.255.255.0 192.168.4.0/255.255.255.0
              Active SAs: 2, origin: crypto map
R2#
```

## IKEv1

အခုစစ်ခဲ့တဲ့ output တွေအားလုံးက phase 1 ကိစစ်တဲ့ command တွေဖြစ်ပါတယ်။

Show crypto ipsec sa ကိုသုံးပြီး phase 2 ကိုစစ်ကြည့်ပါမယ်။

```
R2#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: VPN, local addr 196.0.12.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 196.0.13.2 port 500
    PERMIT, flags={}
      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
  -----
  Omitted output
  -----
  local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
  current_peer 196.0.14.4 port 500
    PERMIT, flags={}
      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```

Phase 2 အောင်မြင်တယ်ဆိုရင် encryption packet နဲ့ decryption packet တွေမှ packet amount တွေ မြင်ရပါလိမ့်မယ်။

## Lab 1 Explanation

အခုလုပ်ခဲ့တဲ့ LAB ရဲရည်ရွယ်ချက်ကတော့ IOS router ပေါ်မှာ site to site VPN လုပ်တတ်အောင်ဖြစ်ပါတယ်။

လေ့လာတဲ့အခါမှာလည်း -

Technology point of view ကလေ့လာတဲ့အခါမှာ IPsec ဆိုတာ ဘာလဲ? ESP ဆိုတာ ဘာလဲ? AH ဆိုတာ ဘာလဲ? ဘယ်လို လုပ်ကြသလဲ စတာတွေကို သိဖို့ လိုပါတယ်။ သိအိုရှိအနေးမှာ ရှင်းပြုခဲ့ပြီး ထပ်မရှင်းပြတော့ပါဘူး။ Implementation point of view ကလေ့လာတာကိုပဲ အကျဉ်းချုပ်ပြီး ရှင်းပြပါမယ်။

## IKEv1

Site to site VPN tunnel တည်ဆောက်ဖို့ encryption လုပ်ဖို့အတွက် ISAKMP (Internet Security Association and Key Management Protocol) နဲ့ IPsec ရဲ့ အခန်းကဏ္ဍဟာ အလွန်အင်မတန်မှ အရေးပါလှပါတယ်။

Host နှစ်ခုဟာ IPsec security association တစ်ခု တည်ဆောက်ဖို့ ညီးမှတွေ လုပ်ရပါတယ်။ အဲဒီလို ညီးမှတွေ အောင်မြင်မှသာ tunnel တစ်ခု အောင်မြင်တာဖြစ်ပါ တယ်။ host တစ်ခုနဲ့ တစ်ခု ညီးမှတွေလုပ်ဖို့ IKE (Internet Key Exchange) လိုခေါ်တဲ့ IKE ကို သုံးရပါတယ်။ အဲဒီ IKE မှာ Phase 1 နဲ့ Phase 2 ဆိုပြီး အပိုင်းနှစ်ပိုင်း ပါဝင်ပါတယ်။

Phase 1 ရဲ့တာဝန်ကတော့ tunnel တစ်ခု တည်ဆောက်ပေးဖို့ပဲဖြစ်ပါတယ်။

Phase 2 ရဲ့တာဝန်ကတော့ data protection အတွက် တာဝန်ယူပေးတာဖြစ်ပါတယ်။

IPsec အနေနဲ့ data ထွေ့ secure ဖြစ်အောင် encryption algorithm ကိုသုံးပြီး ကာကွယ်ပါ လိမ့်မယ်။ နောက် authentication, anti-replay service တွေပါ provide လုပ်ပါတယ်။

## IPsec VPN requirement

အခုလုပ်နေတဲ့ Lab 1 site to site VPN တစ်ခုအောင်မြင်စွာ တည်ဆောက်နိုင်ဖို့ လိုအပ်တဲ့ အချက်တွေကို implementation point of view ကနေတစ်ဆင့်ခြင်း ရှင်းပြပါမယ်။

- **Step – 1 Configure IKE (IKE Phase 1)**
- **Step – 2 Configure IPsec (IKE Phase 2, ACLs, Crypto MAP)**

အခုလုပ်ခဲ့တဲ့ LAB မှာ R2 က HQ router ဖြစ်ပြီး၊ ISP ဆီကနေ static IP ရထားပြီး၊ branch office တွေဖြစ်တဲ့ R3 နဲ့ branch office တစ်ခုဖြစ်တဲ့ R4 ကလည်း static IP ရထားပါတယ်။ ရည်ရွယ်ချက်တော့ R3 နဲ့ R4 ရဲ့ နောက်မှာ ရှိတဲ့ 192.168.3.0/24 နဲ့ 192.168.4.0/24 တို့ကနေ HQ router ရဲ့ နောက်မှာ ရှိတဲ့ 192.168.2.0/24 ကို အဆက်သွယ်လုပ်ချင်တာ ဖြစ်ပါတယ်။

## Step – 1 Configure ISAKMP (IKE) - (ISAKMP Phase 1)

ပထာမအဆင့်အနေနဲ့ IPsec အတွက် SA (security association) တည်ဆောက်ပေးရမှာဖြစ် ပါတယ်။ အဲဒီအတွက် IKE အနေနဲ့ VPN peer တွေအချင်းချင်း မဖြစ်မနေ negotiate

## IKEv1

လုပ်ရမှာဖြစ်ပါတယ်။ ဒါကြောင့် step – 1 အနေနဲ့ ISAKMP phase 1 policy အရင် configure လုပ်ရပါတယ်။

```
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
```

**3DES** ဆိုတာကတော့ phase 1 အတွက်သုံးမယ့် encryption method ဖြစ်ပါတယ်။

**MD5** ဆိုတာကတော့ hashing algorithm ဖြစ်ပါတယ်။

**Pre-share** ဆိုတာကတော့ authentication method အနေနဲ့ pre-share key ကို သုံးမယ်လို့ပြောတာ ဖြစ်ပါတယ်။

**Group 2** ဆိုတာကတော့ DH group ကို သတ်မှတ်ပေးတာဖြစ်ပါတယ်။

crypto isakmp key AMS\_KEY address **0.0.0.0 0.0.0.0** ဆိုတာကတော့ remote branch office တွေက တစ်ခုထက်မကလည်းရှိနေမယ်၊ password ကလည်း တူနေမယ်ဆိုရင် တစ်ကြောင်းတည်းနဲ့ အဆင်ပြေအောင် ဘယ် IP လာလာ လက်ခံမယ်လို့ ပြောလိုက်တာ ဖြစ်ပါတယ်။ ဘယ် router နဲ့ပဲဖြစ်ဖြစ် negotiate လုပ်မယ်လို့ပြောတာဖြစ်ပါတယ်။ ဒါကြောင့် ဘယ် IP နဲ့ပဲ negotiate လုပ်မယ်ဆိုပြီး မသတ်မှတ်တော့ပဲ၊ router အားလုံး တန်ည်းအားဖြင့် ဘယ် IP ဖြစ်ဖြစ်ဆိုတဲ့ အမိပါယ်အနေနဲ့ 0.0.0.0 0.0.0.0 လို့ ရေးပေးရတာ ဖြစ်ပါတယ်။

## Step – 2 Configure IPSec (ISAKMP Phase 2, ACLs, Crypto MAP)

ဒီအဆင့်မှာတော့

- Create extended ACL
- Create IPsec Transform
- Create Dynamic Crypto Maps
- Apply crypto map to the public interface တို့ပါဝင်ပါတယ်။

## IKEv1

VPN tunnel ထဲကနေ ဘယ် traffic တွေကို ဖြတ်သွားခွင့်ပေးမှုလဲဆိတ် သတ်မှတ်ပေးဖို့ extended access-list ရေးပေးဖို့လိုပါတယ်။ ဒါကိုပဲ crypto access-list လို့ခေါ်ကြသလို interesting traffic access-list လို့လည်း ခေါ်ကြပါတယ်။ HQ ဘက်ကနေကြည့်ရင် tunnel နှစ်ခုရှိတဲ့အတွက် သက်ဆိုင်ရာ tunnel အလိုက် ခွဲပြီး ရေးပေးရမှာဖြစ်ပါတယ်။

```
ip access-list extended R2_TO_R3
 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
ip access-list extended R2_TO_R4
 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255
```

Tunnel ထဲကနေ ဖြတ်သွားမယ့် traffic တွေ secure ဖြစ်အောင်၊ data protection အတွက် ISAKMP policy တစ်ခုရေးပေးရမှာဖြစ်ပါတယ်။ ဒါ phase 2 မှာတော့ phase 1 မှာတုန်းကလိုတစ်ခုခြင်းစိ ခွဲမရေးတော့ပဲ တစ်စုစုတစ်စည်းတည်း ရေးပေးနိုင်ပါတယ်။ ဒါကိုတော့ transform set လို့ခေါ်ပါတယ်။

```
crypto ipsec transform-set AMS_SET esp-3des esp-md5-hmac
```

Esp-3des ဆိုတာကတော့ encryption method ဖြစ်ပြီး၊ md5 ကတော့ hashing algorithm ဖြစ်ပါတယ်။

နောက်ဆုံးအဆင့်ကတော့ Crypto map ဖြစ်ပါတယ်။ ရှေ့မှာ လုပ်ခဲ့တဲ့ ISAKMP တို့၊ IPsec တို့နဲ့ပြန်လည်ချိတ်ဆက်ဖို့ crypto map create လုပ်ပေးရမှာဖြစ်ပါတယ်။ လုပ်တဲ့အခါမှာလည်း remote peer က နှစ်ခုဖြစ်တဲ့အတွက် နှစ်ခု သတ်မှတ်ပေးဖို့လိုပါတယ်။

```
crypto map AMS_VPN 10 ipsec-isakmp
 set peer 196.0.13.3
 set transform-set AMS_SET
 match address R2_TO_R3
 crypto map AMS_VPN 11 ipsec-isakmp
 set peer 196.0.14.4
 set transform-set AMS_SET
 match address R2_TO_R4
```

Crypto map name က AMS\_VPN လိုပေးလိုက်ပါတယ်။ အားလုံးပြီးသွားတဲ့အခါ crypto map ကို ISP နဲ့ချိတ်ဆက်ထားတဲ့ interface အောက်မှာ apply လုပ်လိုက်ပါတယ်။

## IKEv1

```
interface FastEthernet0/0
crypto map AMS_VPN
```

ဒါဆိုရင် HQ router မှာ အားလုံးပြီးသွားပါပြီ။ branch office တွေလည်း နားလည်လောက်ပြီ လို့ မျှော်လင့်ပါတယ်။

## NAT and site to site VPN

အကယ်၍ Router တစ်လုံးထဲမှာပဲ internet လည်းသုံးမယ်၊ site to site VPN လည်း သုံးမယ်ဆိုရင်တော့ သတိထားရမယ့်အချက်တွေရှိပါတယ်။ အဲဒါကတော့ NAT packet နဲ့ VPN packet နှစ်ခု ရောထွေးမသွားဖို့ပါပဲ။ order of operation ကိုနားလည်ဖို့လိုပါတယ်။ ဥပမာအနေနဲ့ HQ router R2 မှာ လုပ်ပြပါမယ်။

### R2 NAT Configuration

```
R2(config)#int fa0/0
R2(config-if)#ip nat outside
R2(config-if)#int 10
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#ip access-list extended NAT_ACL
R2(config-ext-nacl)# permit ip 192.168.2.0 0.0.0.255 any
R2(config)#ip nat inside source list NAT_ACL interface
fastethernet0/0 overload
```

အခုံရင် R2 ရဲ့ loopback 0 အနေနဲ့ internet သုံးလို့ရပါပြီ။ internet အနေနဲ့ simulate လုပ်ထားတဲ့ 8.8.8.8 ကို ping ကြည့်ပါမယ်။

```
R2#ping 8.8.8.8 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/62/72 ms
R2#show ip nat translation
Pro Inside global           Inside local          Outside local        Outside global
icmp 196.0.12.2:14         192.168.2.1:14      8.8.8.8:14          8.8.8.8:14
R2#
```

R2 ရဲ့ loopback 0 ဟာ အင်တာနက်သုံးလို့ရနေပါပြီ။

VPN အချင်းချင်းရော pingလို့ရသေးရဲ့လား စမ်းကြည့်ပါ။

## IKEv1

```
R2#ping 192.168.3.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
UUUUU
Success rate is 0 percent (0/5)
R2#
R2#ping 192.168.4.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
UUUUU
Success rate is 0 percent (0/5)
R2#
```

NAT configuration လုပ်ပြီးသွားတဲ့အခါ VPN source အချင်းချင်း ping လို့မရတော့ပါဘူး။  
tunnel up သေးရဲ့လား စစ်ကြည့်ပါ။

```
R2#show crypto isakmp sa
dst          src          state      conn-id slot status
196.0.14.4   196.0.12.2   QM_IDLE    2        0 ACTIVE
196.0.13.3   196.0.12.2   QM_IDLE    1        0 ACTIVE
R2#
```

Tunnel က အောင်မြင်စွာနဲ့ up နေတုန်းပါပဲ။ tunnel up ပါလျှင် ဘာကြောင့် ping လို့မရတာလဲ ဆိုတော့ 192.168.2.1 ကနေ 192.168.3.1 ကိုသွားတာပဲဖြစ်ဖြစ်၊ 192.168.2.1 ကနေ 192.168.4.1 ကိုသွားတာပဲဖြစ်ဖြစ်၊ NAT က ဦးအောင် translate လုပ်ပြီး အင်တာနက်ပေါ် သွားရာနေလိုပြစ်ပါတယ်။ အင်တာနက်ပေါ်မှာ 192.168.3.0/24 လည်းမရှိသလို၊ 192.168.4.0/24 လည်းမရှိပါဘူး။ internet ပေါ်မှာ public IP (global IP) တွေပဲ ရှိပါတယ်။ ဒီပြဿနာကိုဖြေရှင်းဖို့ NAT အတွက် ရေးထားတဲ့ access-list ထဲမှာ VPN အချင်းချင်း သွားမယ့် packet တွေဆိုရင် translate မလုပ်နဲ့ဆိုပြီး deny လုပ်ပေးရမှာဖြစ်ပါတယ်။

## IKEv1

```
R2#sh access-lists
Extended IP access list NAT_ACL
    10 permit ip 192.168.2.0 0.0.0.255 any (3 matches)
Extended IP access list R2_TO_R3
    10 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 (32 matches)
Extended IP access list R2_TO_R4
    10 permit ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255
    20 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255 (18 matches)
R2#
```

```
R2(config)#ip access-list extended NAT_ACL
```

```
R2(config-ext-nacl)#5 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
```

```
R2(config-ext-nacl)#6 deny ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255
```

```
R2#show access-lists
Extended IP access list NAT_ACL
    ⑤ deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
    ⑥ deny ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255
    10 permit ip 192.168.2.0 0.0.0.255 any (3 matches)
Extended IP access list R2_TO_R3
    10 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 (32 matches)
Extended IP access list R2_TO_R4
    10 permit ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255
    20 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255 (18 matches)
R2#
```

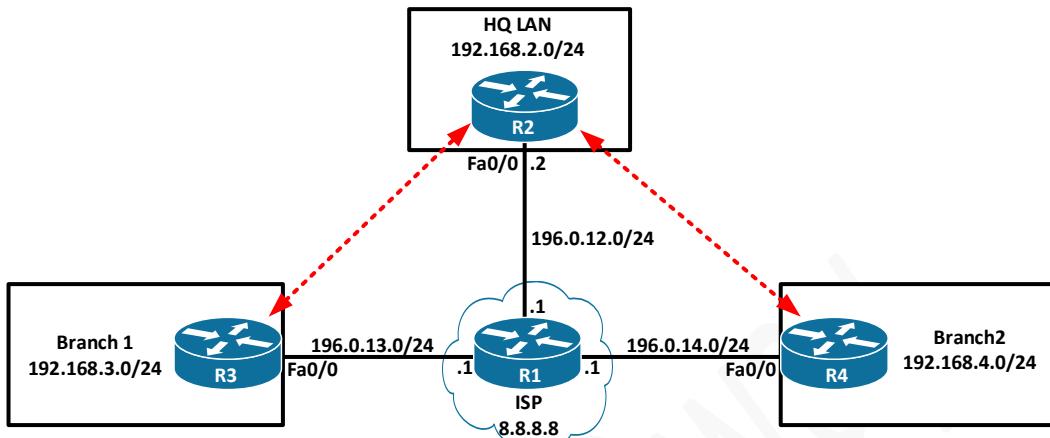
ဖြန့်ပြီး Ping ကြည့်ပါ။

```
R2#p 192.168.3.1 so 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/124/136 ms
R2#p 192.168.4.1 so 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/134/140 ms
R2#ping 8.8.8.8 so 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/66/88 ms
R2#
```

အခုခိုရင် VPN အချင်းချင်းလည်း ping လို့ရသလို၊ internet လည်း သုံးလို့ရနေပါပြီ။

## LAB 2 Site-To-Site VPN with Dynamic IP address (IOS to IOS)

### Diagram



### Task

- Configure site to site VPN between HQ and branch office 1 so that 192.168.2.0/24 and 192.168.3.0/24 communicate each other over the VPN tunnel. Ensure that all users can use internet as well.
- Configure site to site VPN between HQ and branch office 2 so that 192.168.2.0/24 and 192.168.4.0/24 communicate each other over the VPN tunnel. Ensure that all users can use internet as well.
- Branch office 1 and branch office 2 internet edge routers will get dynamic IP from their ISP.
- Use the following policy:

<b>ISAKMP Policy</b>	<b>IPsec Policy</b>
<b>Authentication: Pre-shared</b> <b>Encryption: 3DES</b> <b>Hash: MD5</b> <b>DH Group: 2</b> <b>PSK: AMS_KEY</b>	<b>Encryption: ESP-3DES</b> <b>Hash:MD5</b> <b>Crypto ACL:</b> <b>192.168.2.0/24 &lt;- -&gt; 192.168.3.0/24</b> <b>192.168.2.0/24 &lt;- -&gt; 192.168.4.0/24</b>

**Lab 2 Solution**
**ISP**

```
R1(config)#hostname ISP
ISP(config)#int fa0/0
ISP(config-if)#description ISP_TO_R2
ISP(config-if)#ip add 196.0.12.1 255.255.255.0
ISP(config-if)#no shut
ISP(config-if)#int fa0/1
ISP(config-if)#no shut
ISP(config-if)#description ISP_TO_R3
ISP(config-if)#ip add 196.0.13.1 255.255.255.0
ISP(config-if)#int fa1/0
ISP(config-if)#no shut
ISP(config-if)#description ISP_TO_R4
ISP(config-if)#ip add 196.0.14.1 255.255.255.0
ISP(config-if)#exit
ISP(config)#ip dhcp pool FOR_R3
ISP(dhcp-config)#network 196.0.13.0 255.255.255.0
ISP(dhcp-config)#default-router 196.0.13.1
ISP(dhcp-config)#default-router 196.0.13.1
ISP(dhcp-config)#exit
ISP(config)#int 10
ISP(config-if)#ip add 8.8.8.8 255.255.255.255
```

**R2 Basic Configuration**

```
R2(config)#int fa0/0
R2(config-if)#no shut
R2(config-if)#description R2_TO_ISP
R2(config-if)#ip add 196.0.12.2 255.255.255.0
R2(config-if)#int 10
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#ip route 0.0.0.0 0.0.0.0 196.0.12.1
```

**R3 Basic Configuration**

```
R3(config)#int fa0/0
R3(config-if)#no shut
R3(config-if)#description R3_TO_ISP
R3(config-if)#ip add dhcp
R3(config-if)#int 10
R3(config-if)#ip add 192.168.3.1 255.255.255.0
```

**R4 Basic Configuration**

```
R4(config)#int fa0/0
R4(config-if)#no shut
R4(config-if)#description R4_TO_ISP
R4(config-if)#ip add 196.0.14.4 255.255.255.0
R4(config-if)#int 10
```

## IKEv1

```
R4(config-if)#ip add 192.168.4.1 255.255.255.0
R4(config-if)#ip route 0.0.0.0 0.0.0.0 196.0.14.1
```

### Verification

```
R3#show ip int bri | ex unas
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    196.0.13.2      YES DHCP   up           up
Loopback0          192.168.3.1    YES manual up           up
R3#show ip route static
S*  0.0.0.0/0 [254/0] via 196.0.13.1
R3#
```

အခဲ့ခိုင် R3 မှာ ISP DHCP server ဆီကနေ IP တစ်ခုနဲ့ default route တစ်ခုကြောင်းရနေပါပြီ။ R2, R3, R4 အချင်းချင်း connectivity ရှု မရ ping ကြည့်ပါမယ်။

```
R2#ping 196.0.13.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.0.13.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/109/128 ms
R2#ping 196.0.14.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.0.14.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/104/128 ms
R2#
```

## IPsec Site to Site VPN Configuration

R2	<pre>R2(config)#crypto isakmp policy 10 R2(config-isakmp)# encr 3des R2(config-isakmp)# hash md5 R2(config-isakmp)# authentication pre-share R2(config-isakmp)# group 2 R2(config-isakmp)# lifetime 86400 R2(config-isakmp)#exit R2(config)#<b>crypto isakmp key AMS_KEY address 0.0.0.0 0.0.0.0</b>  R2(config)#ip access-list extended R2_TO_R3 R2(config-ext-nacl)# permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 R2(config-ext-nacl)#ip access-list extended R2_TO_R4 R2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255 R2(config)#crypto ipsec transform-set AMS_SET esp-3des esp-md5-hmac</pre>
----	---

## IKEv1

```
R2 (cfg-crypto-trans)#exit
R2 (config)#crypto map VPN 1 ipsec-isakmp dynamic AMS_VPN
R2 (config)# crypto dynamic-map AMS_VPN 10
R2 (config-crypto-map)# set security-association lifetime
seconds 86400
R2 (config-crypto-map)# set transform-set AMS_SET
R2 (config-crypto-map)# match address R2_TO_R3
R2 (config-crypto-map)#crypto dynamic-map AMS_VPN 11
R2 (config-crypto-map)# set security-association lifetime
seconds 86400
R2 (config-crypto-map)# set transform-set AMS_SET
R2 (config-crypto-map)# match address R2_TO_R4
R2 (config-crypto-map)#exit

R2 (config)#int fa0/0
R2 (config-if)#crypto map VPN
R2 (config-if)#
*Mar 1 00:39:24.603: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

## R3

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)# encr 3des
R3(config-isakmp)# hash md5
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# lifetime 86400
R3(config-isakmp)#crypto isakmp key AMS_KEY address
196.0.12.2
R3(config)#ip access-list extended R3_TO_R2
R3(config-ext-nacl)# permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
R3(config-ext-nacl)#crypto ipsec transform-set AMS_SET esp-3des
esp-md5-hmac
R3(cfg-crypto-trans)#crypto map AMS_VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R3(config-crypto-map)# set peer 196.0.12.2
R3(config-crypto-map)# set transform-set AMS_SET
R3(config-crypto-map)# match address R3_TO_R2
R3(config-crypto-map)#interface FastEthernet0/0
R3(config-if)# crypto map AMS_VPN
R3(config-if)#
*Mar 1 00:40:33.007: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

## IKEv1

**R4**

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)# encr 3des
R4(config-isakmp)# hash md5
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)# lifetime 86400
R4(config-isakmp)#crypto isakmp key AMS_KEY address
196.0.12.2
R4(config)#ip access-list extended R4_TO_R2
R4(config-ext-nacl)# permit ip 192.168.4.0 0.0.0.255
192.168.2.0 0.0.0.255
R4(config-ext-nacl)#crypto ipsec transform-set AMS_SET esp-3des esp-md5-hmac
R4(cfg-crypto-trans)#crypto map AMS_VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R4(config-crypto-map)# set peer 196.0.12.2
R4(config-crypto-map)# set transform-set AMS_SET
R4(config-crypto-map)# match address R4_TO_R2
R4(config-crypto-map)#interface FastEthernet0/0
R4(config-if)# crypto map AMS_VPN
*Mar 1 00:40:49.255: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R4(config-if) #
```

```
R2#show crypto isakmp sa
dst          src          state          conn-id slot status
R2#show crypto ips sa
R2#show crypto session
R2#
```

သာ Tunnel မှာ မတွေ့ရသေးပါဘူး။ ဘာကြောင့်လဲဆိုတော့ site to site vpn ခဲ့သကောက dialer connection လိုမျိုးပဲ traffic စပိုပြီး initiate လုပ်ကြည့်ရပါတယ်။ ဒါမှာ tunnel up မှာ ဖြစ်ပါတယ်။ **အဲဒီလို traffic စပိုတဲ့အခါမှာလည်း dynamic site to site vpn tunnel ဖြစ်တဲ့အတွက် remote site ကနေစရမှာဖြစ်ပါတယ်။ remote site ကသာ စပြီး initiate လုပ်ရပါတယ်။**

## IKEv1

### Verification

```
R3#ping 192.168.2.1 so 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 100/108/120 ms
R3#ping 192.168.2.1 so 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/140/156 ms
R3#
```

```
R4#ping 192.168.2.1 so 10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 100/103/112 ms
R4#ping 192.168.2.1 so 10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/132/136 ms
R4#
```

```
R2#show crypto isakmp sa
dst          src          state      conn-id slot status
196.0.12.2   196.0.13.2   QM_IDLE    1        0 ACTIVE
196.0.12.2   196.0.14.4   QM_IDLE    2        0 ACTIVE

R2#
```

```
R2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
      K - Keepalives, N - NAT-traversal
      X - IKE Extended Authentication
      psk - Preshared key, rsig - RSA signature
      renc - RSA encryption

C-id Local          Remote          I-VRF      Status Encr Hash Auth DH Lifetime Cap.
1    196.0.12.2     196.0.13.2     ACTIVE  3des md5  psk  2   23:39:23
      Connection-id:Engine-id = 1:1(software)
2    196.0.12.2     196.0.14.4     ACTIVE  3des md5  psk  2   23:47:35
      Connection-id:Engine-id = 2:1(software)

R2#
```

## IKEv1

```
R2#show crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 196.0.13.2 port 500
    IKE SA: local 196.0.12.2/500 remote 196.0.13.2/500 Active
    IPSEC FLOW: permit ip 192.168.2.0/255.255.255.0 192.168.3.0/255.255.255.0
                  Active SAs: 2, origin: dynamic crypto map

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 196.0.14.4 port 500
    IKE SA: local 196.0.12.2/500 remote 196.0.14.4/500 Active
    IPSEC FLOW: permit ip 192.168.2.0/255.255.255.0 192.168.4.0/255.255.255.0
                  Active SAs: 2, origin: dynamic crypto map

R2#
```

```
R2#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: VPN, local addr 196.0.12.2

    protected vrf: (none)
    local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
    current_peer 196.0.13.2 port 500
        PERMIT, flags={}
        #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
        #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    -----
    Omitted output
    -----
    local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
    current_peer 196.0.14.4 port 500
        PERMIT, flags={}
        #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
        #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```

## Lab 2 Explanation

အခုလုပ်ခဲ့တဲ့ LAB ရဲ့ရည်ရွယ်ချက်ကတော့ HQ မှာ ISP ဆီက static IP ရထားပြီး၊ branch office တွေမှာ အကြောင်းအမျိုးမျိုးကြောင့် ISP ဆီကနေ static IP မရပဲ၊ dynamic IP ပဲ ရခဲ့ရင် dynamic site to site VPN လုပ်တတ်အောင် ဖြစ်ပါတယ်။

Lab 1 မှာ ရှင်ပြခဲ့တာကိနားလည်ရင် ဒါ Lab 2 လည်းနားလည်ပါပြီ။ တစ်ခုပဲထူးပါတယ်။ အဲဒါကတော့ HQ router မှာ crypto map ဆောက်တဲ့အခါမှာ peer တွေက dynamic IP

## IKEv1

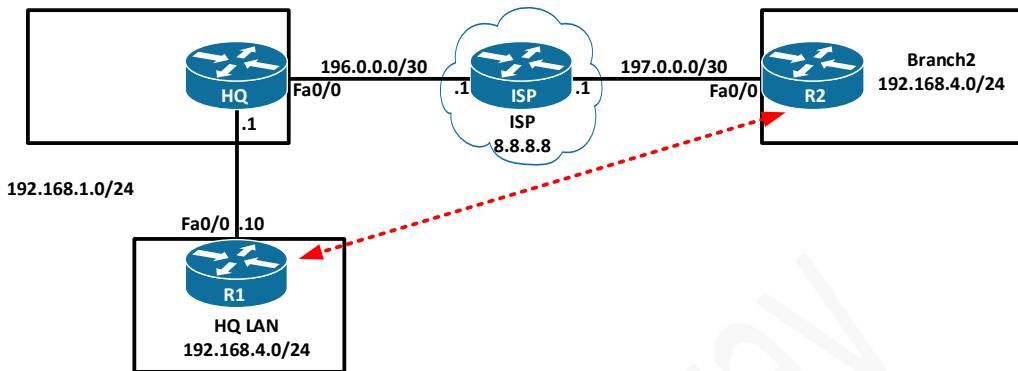
ရုတေသနအတွက် dynamic crypto map ဆောက်ပေးရပါတယ်။ ကျန်တာအားလုံး အတွတ်ပါပဲ။

```
R2(config)#crypto map VPN 1 ipsec-isakmp dynamic AMS_VPN
```

```
R2(config)# crypto dynamic-map AMS_VPN 10
```

## Lab 3 Site-To-Site VPN with NAT-T

### Diagram



### Task

- Configure IPsec site to site VPN on R1 and R2.
- Configure NAT on HQ so that R1 can setup IPsec VPN using policy 10.
- Use following policy:
- Use the following policy:

ISAKMP Policy	IPsec Policy
<b>Authentication: Pre-shared</b> <b>Encryption: AES</b> <b>Hash: Sha</b> <b>DH Group: 5</b> <b>PSK: AMS_KEY</b>	<b>Encryption: ESP-3DES</b> <b>Hash: Sha</b> <b>Crypto ACL:</b> <b>192.168.1.0/24 &lt;- -&gt; 192.168.2.0/24</b> <b>192.168.4.0/24 &lt;- -&gt; 192.168.2.0/24</b>

### Solution

```

HQ
HQ(config)#interface FastEthernet0/0
HQ(config-if)# ip address 196.0.0.2 255.255.255.252
HQ(config-if)# ip nat outside
HQ(config-if)#interface FastEthernet0/1
HQ(config-if)# ip address 192.168.1.1 255.255.255.0
HQ(config-if)# ip nat inside

```

## IKEv1

```

HQ(config)#ip nat inside source list NAT_ACL interface
FastEthernet0/0 overload
HQ(config)#ip nat inside source static udp 192.168.1.10 4500
interface FastEthernet0/0 4500
HQ(config)#ip nat inside source static udp 192.168.1.10 500
interface FastEthernet0/0 500

HQ(config)#ip access-list extended NAT_ACL
HQ(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 any
HQ(config-ext-nacl)#exit

HQ(config)#ip route 0.0.0.0 0.0.0.0 196.0.0.1

```

### R1

```

R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
R1(config)#access-list 101 permit ip 192.168.4.0 0.0.0.255
192.168.2.0 0.0.0.255

R1(config)#crypto isakmp policy 10
R1(config-isakmp)# encr aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# lifetime 43200

R1(config)#crypto isakmp key 6 AMS_KEY address 197.0.0.2
R1(config)#crypto ipsec transform-set AMS_SET esp-3des esp-
sha-hmac
R1(config-crypto-map)# set peer 197.0.0.2
R1(config-crypto-map)# set transform-set AMS_SET
R1(config-crypto-map)# match address 101

R1(config)#interface Loopback0
R1(config-if)# ip address 192.168.4.1 255.255.255.0
R1(config-if)#interface FastEthernet0/0
R1(config-if)# ip address 192.168.1.10 255.255.255.0
R1(config-if)# crypto map VPN MAP

```

### R2

```

R2(config)#interface Loopback0
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# ip nat inside
R2(config-if)#interface FastEthernet0/0
R2(config-if)# ip address 197.0.0.2 255.255.255.252
R2(config-if)# ip nat outside
R2(config-if)#ip route 0.0.0.0 0.0.0.0 197.0.0.1

```

## IKEv1

```
R2(config)#ip nat inside source list NAT_ACL interface
FastEthernet0/0 overload

R2(config)#ip access-list extended NAT_ACL
R2(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255
R2(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255
192.168.4.0 0.0.0.255
R2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 any

R2(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255
R2(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255
192.168.4.0 0.0.0.255

R2(config)#crypto isakmp policy 10
R2(config-isakmp)# encr aes
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 5
R2(config-isakmp)# lifetime 43200
R2(config)#crypto isakmp key 6 AMS_KEY address 196.0.0.2

R2(config)#crypto ipsec transform-set AMS_SET esp-3des esp-
sha-hmac
R2(cfg-crypto-trans)#exit
R2(config)#crypto map VPN_MAP 10 ipsec-isakmp
R2(config-crypto-map)# set peer 196.0.0.2
R2(config-crypto-map)# set transform-set AMS_SET
R2(config-crypto-map)# match address 101

R2(config-if)#interface FastEthernet0/0
R2(config-if)# crypto map VPN_MAP
```

## Verification

```
R1#ping 192.168.2.1 so 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/151/192 ms
R1#
```

## IKEv1

```
R1#show crypto isakmp sa
dst          src          state      conn-id slot status
197.0.0.2    192.168.1.10  QM_IDLE   1        0 ACTIVE
```

R1#

```
R1#sh crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 197.0.0.2 port 4500
  IKE SA: local 192.168.1.10/4500 remote 197.0.0.2/4500 Active
  IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
                Active SAs: 4, origin: crypto map

Interface: FastEthernet0/0
Session status: DOWN
Peer: 197.0.0.2 port 500
  IPSEC FLOW: permit ip 192.168.4.0/255.255.255.0 192.168.2.0/255.255.255.0
                Active SAs: 0, origin: crypto map
```

R1#

```
R1#show crypto ipsec sa
interface: FastEthernet0/0
  Crypto map tag: VPN_MAP, local addr 192.168.1.10

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  current_peer 197.0.0.2 port 4500
    PERMIT. flags={origin_is_acl.}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 7, #recv errors 0
```

## Explanation

ဒါ Lab ရဲရည်ရွယ်ချက်ကတော့ အကယ်၍ IPsec device က NAT device ခဲ့နောက်မှာ ရှိနေခဲ့ရင် လုပ်တတ်အောင်လိုဖြစ်ပါတယ်။ ဒါမျိုးလည်း ကျွန်တော် လက်တွေမှုလည်း ကြံခွဲဖူးပါတယ်။ CCIE exam မှုလည်း ကြံခွဲဖူးပါတယ်။ ဒါကြောင့် အရေးကြီး သက်လုံကောင်းစေဖို့ လုပ်ပြလိုက်တာဖြစ်ပါတယ်။

PAT က LAN to LAN IPsec ကို သွားခွင့်ပြုဖို့အတွက် ဘယ်လို config လုပ်ရတယ်ဆိုတာ နားလည်ဖို့ဖြစ်ပါတယ်။ သိသင့်တာလေးတွေ ထပ်ရှင်းပြပါးမယ်။

## IKEv1

VPN configure လုပ်ထားတဲ့ router ကို VPN Gateway လိုခေါ်ပါတယ်။ PAT configure လုပ်ထားတဲ့ router ကို PAT router လို့ အလွယ်မှတ်ရအောင်။ အခုလုပ်နေတဲ့ LAB မှာဆိုရင် HQ က PAT router ဖြစ်ပြီး၊ R1 က VPN gateway router ဖြစ်ပါတယ်။

IOS version 12.2(13)T နဲ့ သူထက်စောပြီးထုတ်ထားတဲ့ VPN Gateway တွေအတွက်ဆိုရင် PAT router က Encapsulating Security Payload (ESP) ကို ခွင့်ပြုဖို့ IPsec passthrough feature လိုအပ်ပါတယ်။

**Note: This feature is known as IPSec through Network Address Translation (NAT) support in [Software Advisory \(registered customers only\)](#) .**

ဒီနေရာမှာ PAT router က Port Forwarding လုပ်ဖို့ လိုပါတယ်မလိုဘူးဆိုတာ ကွဲကွဲပြားပြား သိဖို့ လိုပါတယ်။

PAT ရဲ့နောက်မှာရှိတဲ့ local peer (in this case R1) ကနေ tunnel ကို initiate လုပ်မယ်ဆိုရင် PAT router မှာ port forwarding လုပ်စရာ မလိုပါဘူး။

Remote peer (in this case R2) ကနေ tunnel ကို initiate လုပ်မယ်ဆိုရင်တော့ PAT router မှာ Port Forwarding configure လုပ်ဖို့ လိုပါတယ်။

ဥပမာ လုပ်ပြထားတာကို အောက်မှာလေ့လာကြည့်ပါ။

**ip nat inside source static esp inside\_ip interface interface**

**ip nat inside source static udp inside\_ip 500 interface interface 500**

ဒါကတော့ IOS version 12.2(13)T နဲ့ သူထက်စောပြီးထုတ်ထားတဲ့ VPN Gateway တွေအတွက် ဖြစ်ပါတယ်။

IOS version 12.2(13)T နောက်မှ ထုတ်ထားတဲ့ VPN Gateway တွေအတွက်ဆိုရင်တော့ IPSec traffic ကို User Data Protocol (UDP) port 4500 packets ထဲမှာထည့်ပြီး encapsulate လုပ်ပါတယ်။ ဒါ feature ကိုတော့ IPSec NAT Transparency လိုခေါ်ပါတယ်။

## IKEv1

ရွှေ့မှာ ရှင်းပြဲသလိုပဲ အကယ်၍ PAT ရဲ့ နောက်မှုရှိတဲ့ local peer (in this case R1) ကနေ tunnel ကို initiate လုပ်မယ်ဆိုရင် PAT router မှာ port forwarding လုပ်စရာ မလိုပါဘူး။

Remote peer (in this case R2) ကနေ tunnel ကို initiate လုပ်မယ်ဆိုရင်တော့ PAT router မှာ Port Forwarding configure လုပ်ဖို့ လိုပါတယ်။

ဥပမာ လုပ်ပြထားတာကို အောက်မှာလေ့လာကြည့်ပါ။

```
ip nat inside source static udp inside_ip 4500 interface interface 4500
```

```
ip nat inside source static udp inside_ip 500 interface interface 500
```

IPsec NAT Transparency ကို disable လုပ်ချင်တယ်ဆိုရင်တော့ no crypto ipsec nat-transparency udp-encaps ဆိုတဲ့ command ကိုသုံးပြီး disable လုပ်နိုင်ပါတယ်။

အခါ ကျွန်ုတ်လုပ်နေတဲ့ LAB တွေမှာ IOS version 15.4 တွေ ဖြစ်နေပါပြီ။

## Lab 4 Site-To-Site VPN with Aggressive mode (IOS to IOS)

### Diagram



### Task

- Configure site to site VPN between HQ and branch office so that 192.168.2.0/24 and 192.168.3.0/24 communicate each other over the VPN tunnel. Ensure that all user can use internet as well. Use the following policy:

ISAKMP Policy	IPSec Policy
Authentication: Pre- shared Encryption: 3DES Hash: MD5 DH Group: 2	Encryption: ESP-3DES Hash: MD5 Proxy ID: 192.168.2.1 <--> 192.168.3.1

Your solution must use only three messages during IKE Phase 1 SA establishment. Peer authentication should use password of "AMS@CISCO".

## IKEv1

### Lab 4 Solution

#### **ISP**

```
R1(config)#hostname ISP
ISP(config)#int fa0/0
ISP(config-if)#description ISP_TO_R2
ISP(config-if)#ip add 196.0.12.1 255.255.255.0
ISP(config-if)#no shut
ISP(config-if)#int fa0/1
ISP(config-if)#no shut
ISP(config-if)#description ISP_TO_R3
ISP(config-if)#ip add 196.0.13.1 255.255.255.0
ISP(config-if)#exit
ISP(config)#int 10
ISP(config-if)#ip add 8.8.8.8 255.255.255.255
```

#### **R2 Basic Configuration**

```
R2(config)#int fa0/0
R2(config-if)#no shut
R2(config-if)#description R2_TO_ISP
R2(config-if)#ip add 196.0.12.2 255.255.255.0
R2(config-if)#int 10
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#ip route 0.0.0.0 0.0.0.0 196.0.12.1
```

#### **R3 Basic Configuration**

```
R3(config)#int fa0/0
R3(config-if)#no shut
R3(config-if)#description R3_TO_ISP
R3(config-if)#ip add 196.0.13.3 255.255.255.0
R3(config-if)#int 10
R3(config-if)#ip add 192.168.3.1 255.255.255.0
```

## Verification

```
R2#ping 196.0.13.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.0.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/115/128 ms
R2#ping 196.0.14.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.0.14.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/127/152 ms
R2#
```

## IKEv1

### IPsec Site to Site VPN Configuration

**R2**

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# encr 3des
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)#exit

R2(config)#crypto isakmp peer address 196.0.13.2
R2(config-isakmp-peer)#set aggressive-mode client-endpoint
ipv4-address 196.0.13.2
R2(config-isakmp-peer)#set      aggressive-mode      password
AMS@CISCO
R2(config-isakmp-peer)#exit

R2(config)#crypto ipsec transform-set AMS_SET esp-3des esp-
md5-hmac
R2(cfg-crypto-trans)#exit

R2(config)#ip access-list extended R2_TO_R3
R2(config-ext-nacl)# permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255

R2(config)#crypto map AMS_VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R2(config-crypto-map)# set peer 196.0.13.2
R2(config-crypto-map)# set transform-set AMS_SET
R2(config-crypto-map)# match address R2_TO_R3
R2(config-crypto-map)#exit
R2(config)#int fa0/0
R2(config-if)#crypto map AMS_VPN
R2(config-if)#
*Mar 1 00:39:24.603: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

**R3**

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)# encr 3des
R3(config-isakmp)# hash md5
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)#exit
```

## IKEv1

```
R3(config)#crypto isakmp peer address 196.0.12.2
R3(config-isakmp-peer)#set aggressive-mode client-endpoint
ipv4-address 196.0.12.2
R3(config-isakmp-peer)#set      aggressive-mode      password
AMS@CISCO
R3(config-isakmp-peer)#exit

R3(config)#ip access-list extended R3_TO_R2
R3(config-ext-nacl)#  permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
R3(config-ext-nacl)#exit

R3(config)#crypto ipsec transform-set AMS_SET esp-3des esp-md5-hmac
R3(cfg-crypto-trans)#crypto map AMS_VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R3(config-crypto-map)# set peer 196.0.12.2
R3(config-crypto-map)# set transform-set AMS_SET
R3(config-crypto-map)# match address R3_TO_R2
R3(config-crypto-map)#interface FastEthernet0/0
R3(config-if)# crypto map AMS_VPN
R3(config-if)#
*Mar 1 00:40:33.007: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

```
R2#show crypto isakmp sa
dst          src          state          conn-id slot status
R2#show crypto ips sa
R2#show crypto session
R2#
```

သာ Tunnel မှာ မတွေ့ရသေးပါဘူး။ သာကြောင့်လဲဆိုတော့ site to site vpn ရဲ့ သဘောက dialer connection လိုမျိုးပဲ traffic စပိုပြီး initiate လုပ်ကြည့်ရပါတယ်။ ဒါမှသာ tunnel up မှာ ဖြစ်ပါတယ်။

## Verification

```
R2#ping 192.168.3.1 so 192.168.2.1
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/125/136 ms
R2#
```

## IKEv1

```
R2#show crypto isakmp sa
dst          src          state      conn-id slot status
196.0.13.2   196.0.12.2  QM_IDLE   1      0 ACTIVE

R2#
R2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
      K - Keepalives, N - NAT-traversal
      X - IKE Extended Authentication
      psk - Preshared key, rsig - RSA signature
      renc - RSA encryption

C-id Local        Remote       I-VRF     Status Encr Hash Auth DH Lifetime Cap.
1    196.0.12.2   196.0.13.2  ACTIVE   3des md5 psk 2  23:50:30
      Connection-id:Engine-id = 1:1(software)
R2#
R2#show crypto ipsec sa
interface: FastEthernet0/0
  Crypto map tag: AMS_VPN, local addr 196.0.12.2
  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 196.0.13.2 port 500
    PERMIT, flags={origin_is_acl,}
  #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
  #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0
  local crypto endpt.: 196.0.12.2, remote crypto endpt.: 196.0.13.2
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
  current outbound spi: 0x417CC512(1098695954)
  inbound esp sas:
    spi: 0x141B2DA3(337325475)
      transform: esp-3des esp-md5-hmac ,
      in use settings ={Tunnel, }
      conn id: 2001, flow_id: SW:1, crypto map: AMS_VPN
      sa timing: remaining key lifetime (k/sec): (4497127/3475)
      IV size: 8 bytes
      replay detection support: Y
      Status: ACTIVE
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
    spi: 0x417CC512(1098695954)
      transform: esp-3des esp-md5-hmac ,
      in use settings ={Tunnel, }
      conn id: 2002, flow_id: SW:2, crypto map: AMS_VPN
      sa timing: remaining key lifetime (k/sec): (4497127/3465)
      IV size: 8 bytes
      replay detection support: Y
      Status: ACTIVE
  outbound ah sas:
  outbound pcp sas:
R2#
```

## IKEv1

```
R2#show crypto ipsec sa identity

interface: FastEthernet0/0
    Crypto map tag: AMS_VPN, local addr 196.0.12.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer (none) port 500
    DENY, flags={ident_is_root,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 196.0.13.2 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

R2#
```

R2#show crypto engine connections active

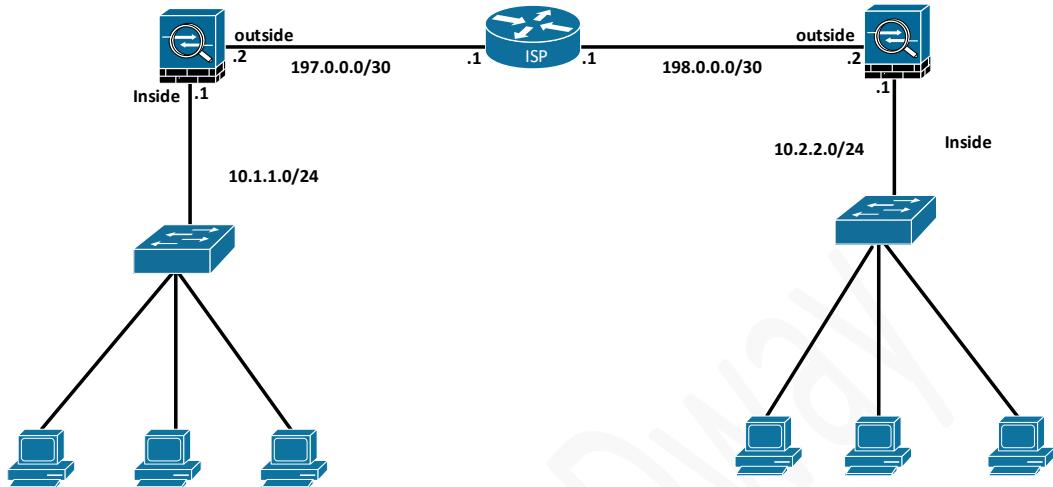
ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0/0	196.0.12.2	set	HMAC_MD5+3DES_56_C	0	0
2001	FastEthernet0/0	196.0.12.2	set	3DES+MD5	0	14
2002	FastEthernet0/0	196.0.12.2	set	3DES+MD5	14	0

R2#

အခုလုပ်ခဲ့တဲ့ LAB ရွှေညွှုယ်ချက်ကတော့ IOS router ပေါ်မှာ site to site VPN မှု  
aggressive mode နဲ့ပက်သက်ပြီး လုပ်တတ်အောင် ဖြစ်ပါတယ်။

## LAB 5 Site-To-Site VPN on ASA 9.7 using IKEv1

### Diagram



### Configuration Steps

1. Enable ISAKMP.
2. Create ISAKMP policy.
3. Set the tunnel type.
4. Define the IPsec policy.
5. Configure the crypto map.
6. Configure traffic filtering (optional).
7. Bypass NAT (optional)
8. Enable Perfect Forward Secrecy (optional).

## IKEv1

### YGN

```
ciscoasa(config)# hostname YGN
YGN(config)# interface gi0/0
YGN(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
YGN(config-if)# ip address 197.0.0.2 255.255.255.252
YGN(config-if)# no shutdown
YGN(config-if)# interface gi0/1
YGN(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
YGN(config-if)# ip address 10.1.1.1 255.255.255.0
YGN(config-if)# no shutdown
YGN(config-if)# exit
YGN(config)# route outside 0.0.0.0 0.0.0.0 197.0.0.1

YGN(config)# crypto ikev1 enable outside
YGN(config)# crypto isakmp identity address

YGN(config)# crypto ikev1 policy 1
YGN(config-ikev1-policy)# authentication pre-share
YGN(config-ikev1-policy)# encryption 3des
YGN(config-ikev1-policy)# hash sha
YGN(config-ikev1-policy)# group 2
YGN(config-ikev1-policy)# lifetime 43200

YGN(config)# crypto ipsec ikev1 transform-set AMS esp-3des
esp-md5-hmac
YGN(config)# access-list VPN_ACL extended permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
YGN(config)# tunnel-group 198.0.0.2 type ipsec-l2l
YGN(config)# tunnel-group 198.0.0.2 ipsec-attributes
YGN(config-tunnel-ipsec)# ikev1 pre-shared-key AMS@VPN
YGN(config-tunnel-ipsec)# crypto map AMS_MAP 1 match
address VPN_ACL
YGN(config)# crypto map AMS_MAP 1 set peer 198.0.0.2
YGN(config)# crypto map AMS_MAP 1 set ikev1 transform-set
AMS
YGN(config)# crypto map AMS_MAP 1 set security-association
lifetime seconds 3600
YGN(config)# crypto map AMS_MAP interface outside
```

## IKEv1

### SG

```

SG(config)# interface gi0/0
SG(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
SG(config-if)# ip address 198.0.0.2 255.255.255.252
SG(config-if)# no shutdown
SG(config-if)# interface gi0/1
SG(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
SG(config-if)# ip address 10.2.2.1 255.255.255.0
SG(config-if)# no shutdown
SG(config-if)# exit
SG(config)# route outside 0.0.0.0 0.0.0.0 198.0.0.1

SG(config)# crypto ikev1 enable outside
SG(config)# crypto isakmp identity address

SG(config)# crypto ikev1 policy 1
SG(config-ikev1-policy)# authentication pre-share
SG(config-ikev1-policy)# encryption 3des
SG(config-ikev1-policy)# hash sha
SG(config-ikev1-policy)# group 2
SG(config-ikev1-policy)# lifetime 43200
SG(config-ikev1-policy)# crypto ipsec ikev1 transform-set
AMS esp-3des esp-md5-hmac
SG(config)# access-list VPN_ACL extended permit ip
10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
SG(config)# tunnel-group 197.0.0.2 type ipsec-l2l
SG(config)# tunnel-group 197.0.0.2 ipsec-attributes
SG(config-tunnel-ipsec)# ikev1 pre-shared-key AMS@VPN
SG(config-tunnel-ipsec)# exit
SG(config)# crypto map AMS_MAP 1 match address VPN_ACL
SG(config)# crypto map AMS_MAP 1 set peer 197.0.0.2
SG(config)# crypto map AMS_MAP 1 set ikev1 transform-set
AMS
SG(config)# crypto map AMS_MAP interface outside

```

### ISP

```

ISP(config)#interface Ethernet0/0
ISP(config-if)# ip address 197.0.0.1 255.255.255.252
ISP(config)#interface Ethernet0/1
ISP(config-if)# ip address 198.0.0.1 255.255.255.252
ISP(config)#interface loopback 0
ISP(config-if)#ip add 8.8.8.8 255.255.255.255

```

## IKEv1

## Verification

```
YGN-PC> show ip

NAME      : YGN-PC[1]
IP/MASK   : 10.1.1.10/24
GATEWAY   : 10.1.1.1
DNS       :
MAC       : 00:50:79:66:68:06
LPORT     : 20000
RHOST:PORT : 127.0.0.1:30000
MTU       : 1500
```

```
YGN-PC>
```

```
SG-PC> sh ip

NAME      : SG-PC[1]
IP/MASK   : 10.2.2.10/24
GATEWAY   : 10.2.2.1
DNS       :
MAC       : 00:50:79:66:68:07
LPORT     : 20000
RHOST:PORT : 127.0.0.1:30000
MTU       : 1500
```

```
SG-PC>
```

```
YGN-PC> ping 10.2.2.10
```

```
84 bytes from 10.2.2.10 icmp_seq=1 ttl=64 time=18.060 ms
84 bytes from 10.2.2.10 icmp_seq=2 ttl=64 time=11.458 ms
84 bytes from 10.2.2.10 icmp_seq=3 ttl=64 time=5.230 ms
84 bytes from 10.2.2.10 icmp_seq=4 ttl=64 time=6.846 ms
84 bytes from 10.2.2.10 icmp_seq=5 ttl=64 time=7.242 ms
```

```
YGN-PC> _
```

## IKEv1

```
YGN# show crypto isakmp sa
```

IKEv1 SAs:

```
Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 198.0.0.2
  Type      : L2L          Role     : initiator
  Rekey     : no           State    : MM_ACTIVE
```

There are no IKEv2 SAs  
YGN#

```
YGN# show crypto isakmp sa detail
```

IKEv1 SAs:

```
Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 198.0.0.2
  Type      : L2L          Role     : initiator
  Rekey     : no           State    : MM_ACTIVE
  Encrypt   : 3des         Hash     : SHA
  Auth      : preshared    Lifetime: 43200
  Lifetime Remaining: 42768
```

There are no IKEv2 SAs  
YGN#

```
YGN# show crypto ipsec sa
interface: outside
Crypto map tag: AMS_MAP, seq num: 1, local addr: 197.0.0.2
access-list VPN ACL extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.255
0
  local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
  current_peer: 198.0.0.2

  #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
  #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
```

## Lab 6 Command Explanation

### Phase 1 configuration

၃ Lab ရဲရည်ရွယ်ချက်ကတော့ အကယ်၍များ ASA ပေါ်မှာ site to site VPN tunnel configure လုပ်ဖို့ကြံလာရင် လုပ်တတိဖို့ဖြစ်ပါတယ်။

Phase 1 ရဲတာဝန်ကတော့ YGNASA နဲ့ SGASA နှစ်ခုအကြား secure tunnel တစ်ခုတည်ဆောက်ပေးရမှာဖြစ်ပါတယ်။ ASA နှစ်လုံးစလုံးက tunnel တစ်ခုတည်ဆောက်ဖို့ အချင်းချင်း secret key exchange ကိစ္စတွေ၊ အချင်းချင်း authentication ကိစ္စတွေ၊ IKE

## IKEv1

security policy နဲ့ပက်သက်ပြီး ညီညွင်းမှတွေ လုပ်ကြပါလိမ့်မယ်။ phase 1 configuration တွေကတော့ အောက်ပါအတိုင်းဖြစ်ပါတယ်။

```
YGN(config)# crypto ikev1 policy 1
YGN(config-ikev1-policy)# authentication pre-share
YGN(config-ikev1-policy)# encryption 3des
YGN(config-ikev1-policy)# hash sha
YGN(config-ikev1-policy)# group 2
YGN(config-ikev1-policy)# lifetime 43200
```

**YGN(config)# crypto ikev1 policy 1**

ဆိတ်ဘကတော့ IKE policy number 1 လို့ပြောတာဖြစ်ပါတယ်။ အကယ်၍ ကိုယ့်မှာ peer တစ်ခုထက်မကရှိနေခဲ့ရင် policy ကလည်း မတူဘူးဆိုရင် policy တွေကို number 1 ,2 , 3 စသဖြင့် ခွဲခြားပေးဖို့ဖြစ်ပါတယ်။ number ထံလေ priority ပိုမြင့်လေဖြစ်ပါတယ်။ နှစ်ဘက်တူစရာမလိုပါဘူး။ တူချင်တူ မတူချင်နေ ကိစ္စမရှိပါဘူး။ ASA version 8.4 မတိုင်ခင်တူန်းက version တွေဆိုရင်တော့ crypto isakmp policy ဆိုတဲ့ command ကိုသုံးပါတယ်။ အခုနောက်ပိုင်း ASA version crypto ikev1 လို့ သုံးပါတယ်။ ikev2 အကြောင်းလည်း နောက်သင်ခန်းစာမှာ လေ့လာရမှာဖြစ်ပါတယ်။

**YGN(config-ikev1-policy)# authentication pre-share**

ဆိတ်ဘကတော့ authentication အတွက် pre-share key ကို သုံးမယ်လို့ပြောတာဖြစ်ပါတယ်။ နှစ်ဘက်စလုံးတူဖို့လိုပါတယ်။

**YGN(config-ikev1-policy)# encryption 3des**

ဆိတ်ဘကတော့ Encryption method 3des ကိုသုံးမယ်လို့ပြောတာဖြစ်ပါတယ်။ နှစ်ဘက်စလုံး တူဖို့လိုပါတယ်။

**YGN(config-ikev1-policy)# group 2**

ဆိတ်ဘကတော့ secret key exchange လုပ်ဖို့အတွက် Diffie-Hellman group 2 ကို သုံးမယ်လို့ပြောတာဖြစ်ပါတယ်။

**YGN(config-ikev1-policy)# lifetime 43200**

ဆိတ်ဘကတော့ security association က 43200 seconds ဖြစ်တယ်လို့ပြောတာဖြစ်ပါတယ်။ expire ဖြစ်သွားတနဲ့ ပြန်ပြီး negotiation ပြန်လုပ်ရမှာဖြစ်ပါတယ်။

**YGN(config)# crypto ikev1 enable outside**

**YGN(config)# crypto isakmp identity address**

## IKEv1

ဒီနှစ်ကြောင်းမှာ ပထမတစ်ကြောင်းကတော့ outside interface ပေါ်မှာ ikev1 ကို enable လုပ်လိုက်တာဖြစ်ပါတယ်။ ဒုတိယတစ်ကြောင်းကတော့ ASA အနေနဲ့ FQDN သုံးတာမဟုတ်ပဲ သူ့ရဲ့ IP ကိုသုံးပြီး သူကိုယ်သူ identify လုပ်တာဖြစ်ပါတယ်။

```
YGN(config)# tunnel-group 198.0.0.2 type ipsec-l2l
YGN(config)# tunnel-group 198.0.0.2 ipsec-attributes
YGN(config-tunnel-ipsec)# ikev1 pre-shared-key AMS@VPN
ဒီသုံးကြောင်းမှာ ပထမတစ်ကြောင်းကတော့ 198.0.0.2 ဆိုတာ peer ဖြစ်တဲ့ SG firewall outside interface ရဲ့ IP ဖြစ်ပါတယ်။ ipsec-l2l ဆိုတာကတော့ Lan to Lan လိုပြောတာဖြစ်ပါတယ်။
```

ဒုတိယတစ်ကြောင်း နဲ့ တတိယတစ်ကြောင်းကတော့ ASA နှစ်ခုအတွက်သုံးမယ့် pre-shared key ကိုသတ်မှတ်ပေးတာဖြစ်ပါတယ်။ pre-shared key ကို AMS@VPN လိုသတ်မှတ်လိုက်ပါတယ်။

အခုရှင်းပြခဲ့တာတွေကတော့ phase - 1 အကြောင်းပဲဖြစ်ပါတယ်။ SG ASA မှာလည်း ဒီအတိုင်းပဲဖြစ်ပါတယ်။ အခုရှင်းပြခဲ့တာကို နည်းမျိုးသိပါ။

### Phase 2 configuration

Phase 1 အောင်မြင်လို့ tunnel up သွားပြီဆိုတာနဲ့ phase 2 လည်း negotiate အလုပ်စလုပ်ပါတယ်။ phase 2 ရဲ့ တာဝန်ကတော့ tunnel ထဲကကနေသွားမယ့် traffic တွေအတွက် secure ဖြစ်အောင် protect လုပ်ပေးရမှာဖြစ်ပါတယ်။

```
YGN(config)# access-list VPN_ACL extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
ဆိုတာကတော့ ဘယ် traffic တွေကို encrypt လုပ်မလဲဆိုတာ သတ်မှတ်ပေးဖို့ ACL ရေးပေးရမှာဖြစ်ပါတယ်။ ဒီဥပမာမှာတော့ 10.1.1.0/24 ကနေ 10.2.2.0/24 ကိုသွားတဲ့အခါ encrypt လုပ်ပါလိမ့်မယ်။
```

```
YGN(config)# crypto ipsec ikev1 transform-set AMS esp-3des esp-md5-hmac
```

ဆိုတာကတော့ peer တွေအနေနဲ့ encryption algorithm နဲ့ authentication algorithm ကို ညီးစွဲလိုပါတယ်။ အဲဒီအတွက် phase 1 တုန်းကလို တစ်ကြောင်းခြင်းစီ မရေးပဲ transform set ဆိုပြီး ပေါင်းရေးလိုက်တာဖြစ်ပါတယ်။ transform set name ကို AMS လိုပေးလိုက်ပါတယ်။ esp-3des က encryption method ဖြစ်ပြီး esp-md5-hmac က authentication method ဖြစ်ပါတယ်။

## IKEv1

```
YGN(config-tunnel-ipsec)# crypto map AMS_MAP 1 match address
VPN_ACL
```

```
YGN(config)# crypto map AMS_MAP 1 set peer 198.0.0.2
```

```
YGN(config)# crypto map AMS_MAP 1 set ikev1 transform-set AMS
```

```
YGN(config)# crypto map AMS_MAP interface outside
```

Transform set ဆောက်ပြီးရင် Phase 2 မှာ ပါဝင်ရမယ့် parameter တွေအားလုံးပါဝင်တဲ့ crypto map တစ်ခုဆောက်ပေးရပါတယ်။ crypto-map name ကို AMS\_MAP လို့ပေးလိုက်ပါတယ်။ sequence number ကို 1 လိုပေးလိုက်ပါတယ်။ အကယ်၍များ ကိုယ့်မှာ peer တွေအများကြီးရှိတယ်ဆိုရင် sequence number တွေခဲ့ပြီး သုံးနိုင်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ peer တွေ ဘယ်လောက်ပဲများများ crypto map တစ်ခုပဲ apply လုပ်လိုဂုဏ်ဖြစ်ပါတယ်။ set peer ဆိုတဲ့ command နဲ့ remote peer ရဲ့ IP ကို သတ်မှတ်ပေးရမှာဖြစ်ပါတယ်။ set ikev1 transform-set ဆိုတဲ့ command နဲ့ ရှေ့မှာ ရေးခဲ့တဲ့ transform name ကို သတ်မှတ်ပေးရမှာဖြစ်ပါတယ်။ set security-association ကိုသုံးပြီး negotiation လုပ်ရမယ့် အချိန်ကို သတ်မှတ်ချင် သတ်မှတ်နိုင်ပါတယ်။ interface command နဲ့ outside interface ပေါ်မှာ crypto map ကို activate လုပ်လိုက်တာဖြစ်ပါတယ်။

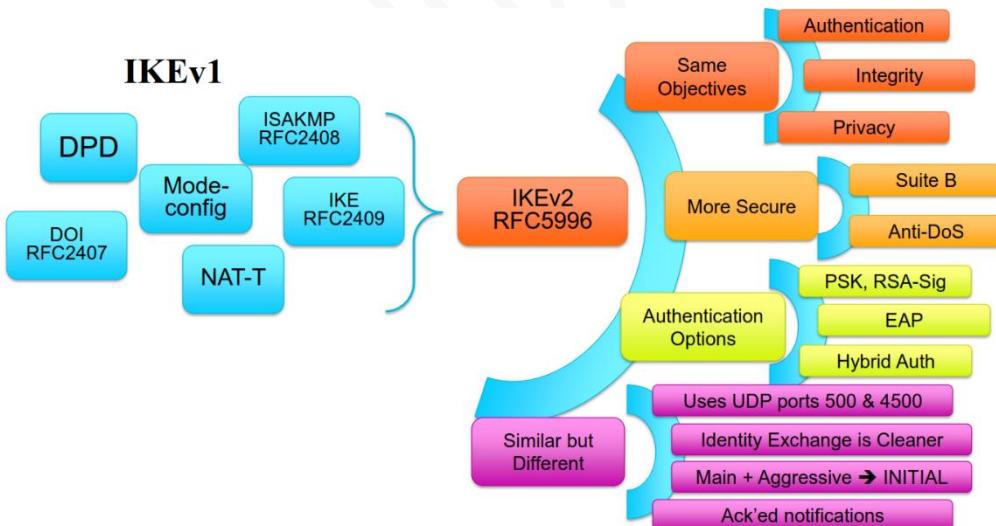
အားလုံးပြီးသွားပြီဆိုရင် end device အချင်းချင်း ping ကြည့်ပါ။ show crypto isakmp sa နှစ်ကြည့်ပါ။ Please 1 အောင်မြင်လား၊ မအောင်မြင်လားဆိုတာ သိနိုင်ပါတယ်။ ဒါ show crypto isakmp sa command ကတော့ phase 1 ကိုစစ်တဲ့ command ဖြစ်ပါတယ်။ show crypto ipsec sa ကတော့ phase 2 ကိုစစ်တဲ့ command ဖြစ်ပါတယ်။ အကယ်၍ phase 2 အောင်မြင်တယ်ဆိုရင် encrypt: နဲ့ decrypt: မှာ packet amount တွေတက်နေတာ မြင်ရပါလိမ့်မယ်။

## Internet Key Exchange Version 2 (IKEv2 IPsec)

### IKEv2 Overview

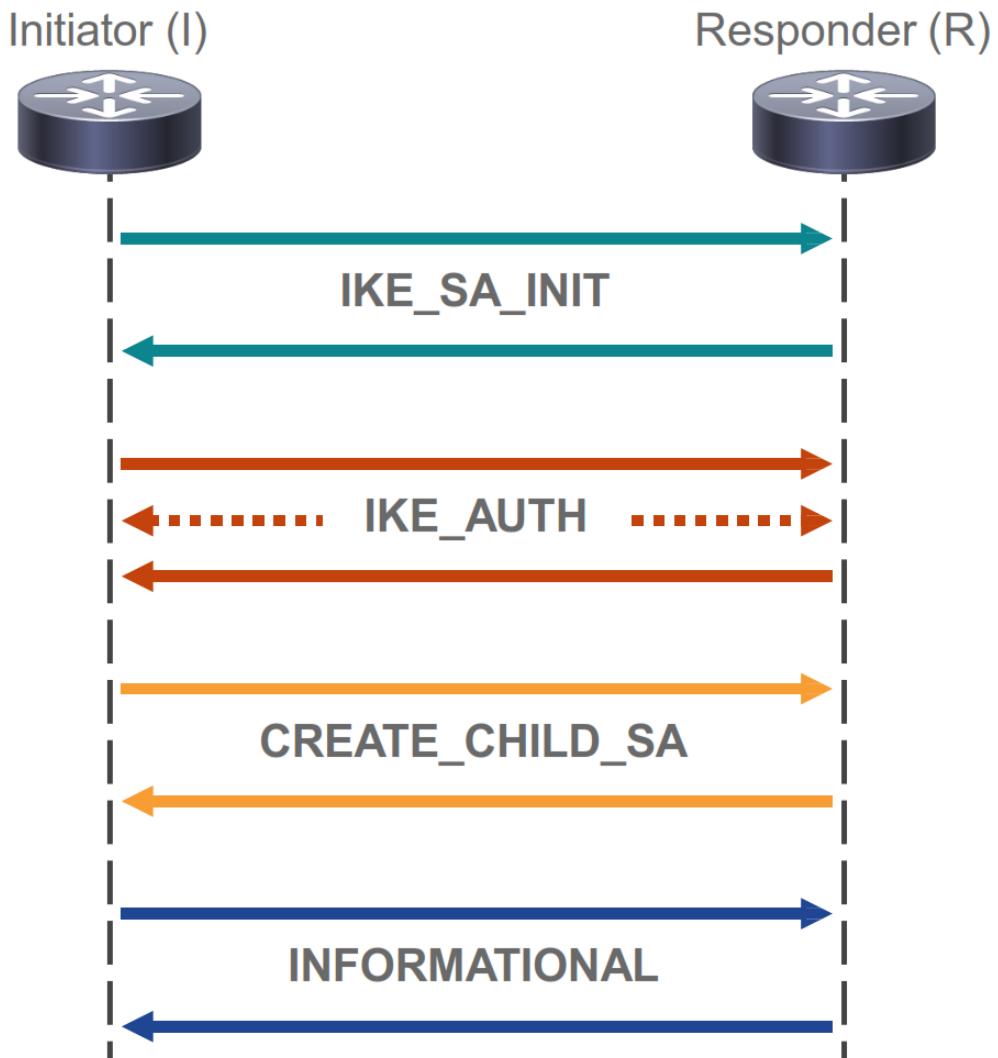
IKEv1 နောက်မှာ ပေါ်လာတဲ့ version ကတေသ့ IKEv2 ဖြစ်ပါတယ်။ IKEv2 မှာတေသ့ အသစ် proposed standard ပါဝင်လာပါတယ်။ message exchange လုပ်တဲ့အခါမှာလည်း IKEv1 လောက်မများတော့တဲ့အတွက် IKEv1 လိုမျိုး overhead မဖြစ်တော့ပါဘူး။ IKEv1 လောက်လည်း မရှုပ်ထွေးတော့ပါဘူး။ **IKEv1 နဲ့မတူတဲ့အချက်တစ်ခုကတေသ့ DoS attack ကိုကာကွယ်ပေးတာပဲဖြစ်ပါတယ်။** သတိထားရမှာတစ်ခုကတေသ့ IKEv1 နဲ့ IKEv2 အချင်းချင်း compatible မဖြစ်တဲ့အတွက် အတူတဲ့ အသုံးပြုလို့ မရပါဘူး။ IKEv2 ဟာ IKEv1 ကို ကောင်းသထ်က ကောင်းသထ်ကောင်းအောင် enhance လုပ်ထားတာဖြစ်ပါတယ်။ ရည်ရွယ်ချက်ကတေသ့ IKEv1 လိုပဲ IPsec ကိုသုံးပြီး user data တွေကို protect လုပ်ပေးဖို့ဖြစ်ပါတယ်။ IKEv2 အကြောင်းကိုတေသ့ RFC 5996 မှာ လေ့လာနိုင်ပါတယ်။ IKEv1 နဲ့ IKEv2 ကွာခြားချက်တွေကို လေ့လာကြည့်ပါ။

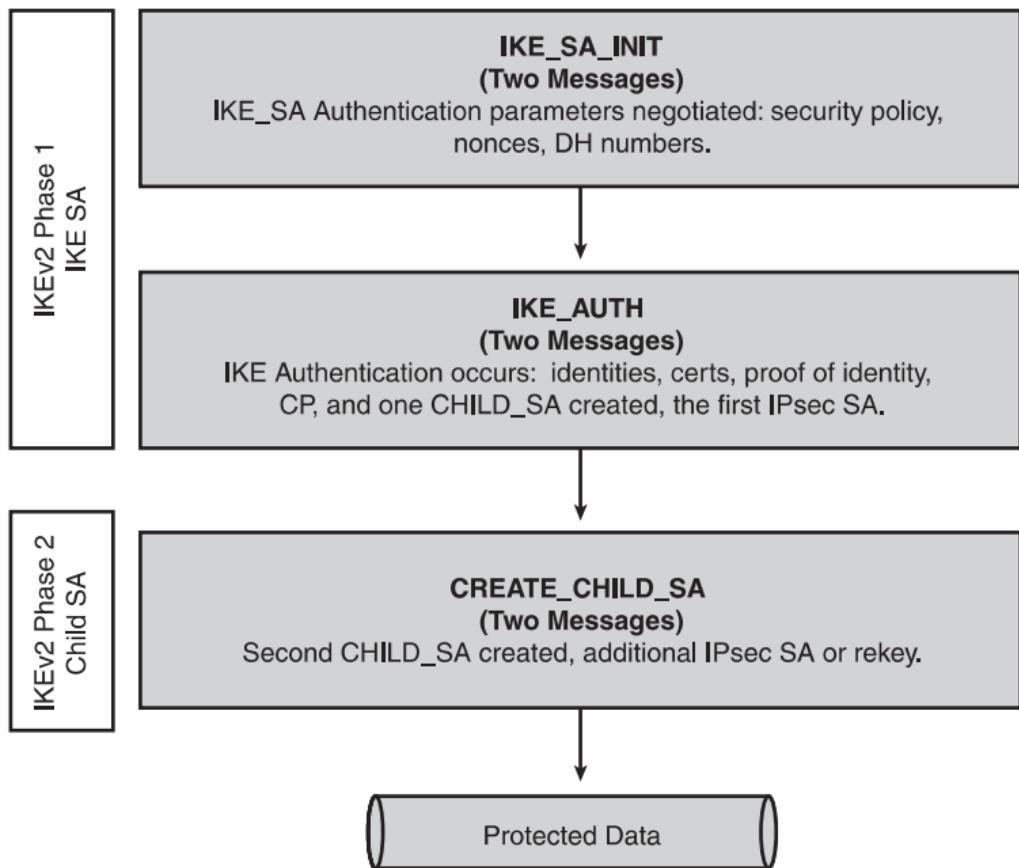
### Comparing IKEv1 and IKEv2



## IKEv2

	IKEv1	IKEv2
Auth messages	6 max	Open ended
First IPsec SA	9 msgs min	~ 4-6 msgs min
Authentication	pubkey-sig, pubkey-encr, PSK	Pubkey-sig, PSK, <b>EAP</b>
Anti-DOS	Never worked	Works!
IKE rekey	Requires re-auth (expensive)	No re-auth
Notifies	Fire & Forget	Acknowledged





IKEv1 နဲ့ IKEv2 နှင့်ယူပြထားတဲ့ Table 0 – 1 ကိုလည်းလေ့လာကြည့်ပါ။

	<b>IKEv1</b>	<b>IKEv2</b>
UDP Port	500	500,4500
Phases	Phase 1 (6/3 messages) Phase 2 (3 messages)	Phase 1 (4 messages) Phase 2 (2 messages)
Keepalives	No	Yes
SA Negotiation	Responder selects initiator's proposal	Same as IKEv1, proposal structure simplified
Number of Msgs	6 – 9	4 – 8
EAP/CP	No	Yes

**Table 0 – 1**

## IKEv2

IKEv2 မှ ပထမအဆင့်အနေနဲ့ initial handshake ပါဝင်ပါတယ်။ initial handshake ကို **IKE\_SA\_INIT or initial exchange** လိုခေါ်ပါတယ်။ ဒီအဆင့်မှာ IKEv2 tunnel တည်ဆောက်ရာမှာ ပါဝင်တဲ့ device နှစ်ခုဟာ အသုံးပြုမယ့် cryptographic algorithm တွေကို negotiate လုပ်ရပါတယ်။ Diffie-Hellman (DH) public value ကို exchange လုပ်ရပါတယ်။ အချုပ်အားဖြင့်မှတ်မယ်ဆိုရင်တော့ proposal selection, key exchange စုံပါဝင်ပါတယ်။

ဒုတိယအဆင့်ကတော့ **IKE\_AUTH or authentication** ဖြစ်ပါတယ်။ ဒီအဆင့်မှာတော့ identity exchange လုပ်တာတွေ၊ အပြန်အလှန် authentication လုပ်တာတွေ၊ initial IPsec SAs establishment တွေပါဝင်ပါတယ်။ optional အနေနဲ့ certificate exchange and configuration exchange လည်း ပါဝင်ပါတယ်။ Additional IPsec Security Association တွေကိုတော့ **Child SAs** လိုခေါ်ပါတယ်။

IKEv2 မှ ရွေးကြီးကြီးပေးဝယ်ထားရတဲ့ resource တွေကို waste ဖြစ်အောင် လုပ်မယ့် spoofing attack တွေကို လျှော့ချို့အတွက် denial of service (DoS) attack protection mechanism လည်းပါဝင်ပါတယ်။

IKEv2 message exchange လုပ်တဲ့အခါ request/response pairs ပါဝင်ပါတယ်။ အကယ်၍ reply ပြန်မလာရင် request လုပ်တဲ့ sender အနေနဲ့ message ကို retransmit ပြန်လုပ်ရပါတယ်။

IKEv2 SA ဘာ complete ဖြစ်သွားတဲ့အခါ INFORMATIONAL message ကို အသုံးပြုပြီး additional control message တွေကို exchange လုပ်နိုင်ပါတယ်။

- IKEv2 မှာ NAT traversal ကို built-in support လုပ်ပါတယ်။ IPsec peer ၏ NAT router ရဲ့နောက်မှုရှိနေရင် NAT-T လိုအပ်ပါတယ်။
- IKEv2 မှာ tunnel အတွက် built-in keepalive mechanism ရှိပါတယ်။
- IKEv2 ဘာ IKEv1 လောက် bandwidth ကုန်ဆုံးမှု မရှိပါဘူး။
- IKEv2 ၏ EAP support လုပ်ပြီး IKEv1 တော့ EAP support မလုပ်ပါဘူး။ IKEv2 အနေနဲ့ authentication method သုံးခု support လုပ်ပါတယ်။ PSK, PKI (RSA-Sig),

## IKEv2

EAP (initiator only) တိုဖြစ်ပါတယ်။ initiator ကို client လို့ မှတ်နိုင်ပြီး responder ကိုတော့ server လို့ မှတ်နိုင်ပါတယ်။

- IKEv2 က MOBIKE ကို support လုပ်ပါတယ်။ IKEv1 ကတော့ support မလုပ်ပါဘူး။ (MOBIKE allows IKEv2 to be used in mobile platforms like phones and by users with multi-homed setups.)
- IKEv2 အနေနဲ့ tunnel က alive ဖြစ် မဖြစ် detect လုပ်နိုင်ပါတယ်။ IKEv1 ကတော့ Dead Peer Detection” (DPD) သုံးမှသာ သိနိုင်ပါတယ်။ DPD ဟာ IKEv2 ခဲ့ standard ဖြစ်လာပါတယ်။ ဒါပေမယ့် IOS မှတော့ default က disable ဖြစ်ပါတယ်။ IKEv2 profile အောက်မှာ configure လုပ်နိုင်ပါတယ်။ peer နှစ်ဘက်လုံးမှာ enable လုပ်ဖို့ လိုပါတယ်။
- IKEv2 မှာ acknowledgment and sequence ရှိတဲ့အတွက် reliability ရှိပါတယ်။ ဒါပေမယ့် IKEv1 မှတော့ အဲဒီလို မရှိပါဘူး။
- IKEv2 အနေနဲ့ 4 messages ဲ generate လုပ်ပါတယ်။ အဲဒီ message တွေကတော့ IKE\_SA\_INIT, IKE\_AUTH, CREATE\_CHILD\_SA, နဲ့ Informational တို့ ဖြစ်ပါတယ်။ IKEv1 ကတော့ phase 1 မှာ main mode သုံးထားရင် 6 messages အသုံးပြုပြီး၊ aggressive mode မှတော့ 3 messages ကို အသုံးပြုပါတယ်။ IKEv1 မှ main mode and aggressive mode ဆိုပြီး နှစ်မျိုးရှိပါတယ်။ IKEv2 မှတော့ IKE\_SA\_INIT ဆိုပြီး single function ဲ ရှိပါတယ်။ IKEv1 phase 2 မှာ Quick mode က IKEv2 မှတော့ CREATE\_CHILD\_SA လို့ခေါ်ပါတယ်။
- FlexVPN ဟာ IKEv2 နဲ့ အလုပ်လုပ်ပါတယ်။ IKEv1 နဲ့ အလုပ် မလုပ်ပါဘူး။
- IKEv1 အနေနဲ့ symmetric authentication ဲ support လုပ်ပါတယ်။ IKEv2 ကတော့ symmetric authentication ရော့၊ asymmetric authentication ပါ support လုပ်ပါတယ်။
- IKEv1 policy က IKEv2 မှာ proposal လို့ခေါ်ပါတယ်။
- IKEv2 မှာ built-in Anti-DoS protection mechanism ပါဝင်ပါတယ်။

## IKEv2

IKEv2 နှုပ်သက်ပြီး [RFC 5996](#) မှာလည်း လေ့လာနိုင်ပါတယ်။ IKEv2 tunnel တည်ဆောက်တဲ့အခါ အသုံးပြုတဲ့ အဆင့်တွေကို လေ့လာကြည့်ရအောင်။

### IKEv2 CLI Overview

IKEv2 configuration လုပ်တဲ့အခါ လွှာယ်ကူစေဖို့အတွက် configuration block ကို သိထားသင့်ပါတယ်။ အဆင့်ဆင့် configure လုပ်ပုံကို လေ့လာကြည့်ပါ။

Step – 1 IKEv2 Proposal

Step – 2 IKEv2 Policy binds Proposal to peer

Step – 3 Keyring supports asymmetric PSK's

Step – 4 IKEv2 Authorization Policy (contains attributes for local AAA & config. exchange)

Step – 5 IKEv2 Profile

Step – 6 Crypto IPsec Transform-Set

Step – 7 interface virtual-template 1 type tunnel

Step – 8 interface tunnel 0

### Introducing Smart Defaults

Default value ကိုသုံးပြီး IKEv2 နဲ့ IPsec configuration ကို minimize လုပ်စွဲ Smart default ဆိုတာရှိပါတယ်။ default value ကိုလည်း လိုအပ်သလို ပြင်ဆင်ပါတယ်။ smart default မှာ default IKEv2 proposal, default IKEv2 policy နဲ့ default IPsec profile တို့ပါဝင်ပါတယ်။ အောက်ပါအတိုင်း စစ်ကြည့်နိုင်ပါတယ်။

```
R2#sh crypto ikev2 proposal
IKEv2 proposal: default
    Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
    Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
    PRF         : SHA512 SHA384 SHA256 SHA1 MD5
    DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
R2#
```

## IKEv2

```
R2#show crypto ikev2 policy
```

```
IKEv2 policy : default
    Match fvrdf : any
    Match address local : any
    Proposal      : default
R2#
```

```
R2#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac }
    will negotiate = { Transport, },
R2#
R2#show crypto ipsec profile default
IPSEC profile default
    Security       association      lifetime:        4608000
    kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={

            default: { esp-aes esp-sha-hmac } ,
        }
R2#
```

## Modular building block

Tunneling	Authentication Method	Tunnel Config	Config Mode Source
GRE/IPsec	Certificate	Static	Local config
Pure IPsec	Pre-shared Key	Dynamic	RADIUS
	EAP (initiator)	crypto map	Hybrid

Security policy & routing
IKEv2 "routing"
BGP
Static routes
Reverse-Route Injection
EIGRP or anything else!

<b>IKE V1</b>	<b>IKE V2</b>
1)IKEv1 policy	1a) IKev2 proposal
	1b) IKev2 policy
2)Keying	2a) keying
	2b)IKev2 profile
3)IPsec	3)IPsec
4)interesting ACL	4) ACL
5)Crypto map	5) crypto map
6)Apply to interface	6) apply to interface

### **IKEv2 Proposal**

IKEv2 proposal အနေနဲ့ IKE\_SA\_INIT မှာ negotiate လုပ်ရမယ့် cryptographic transforms တွေကို သတ်မှတ်ပေးပါတယ်။ transform type တွေကတော့ encryption algorithm, pseudorandom function, integrity algorithm, နဲ့ Diffie-Hellman group တို့ဖြစ်ပါတယ်။ IKEv1 နဲ့ မတူတဲ့အချက်ကတော့ IKEv2 အနေနဲ့ authentication method နဲ့ SA lifetime ကို negotiate မလုပ်ပါဘူး။ ဒါကြောင့် IKEv2 configure လုပ်တဲ့အခါ authentication method နဲ့ SA lifetime မပါဝင်ပါဘူး။

IKEv2 proposal တစ်ခုထက်မက configure လုပ်လို့ရသလို့ proposal တစ်ခုမှာလည်း transform type တစ်ခုထက်မကပါလို့ ရပါတယ်။ ကိုယ်အသုံးပြုချင်တဲ့ transform type တွေကိုပဲ သက်သက်စုပြီး အသုံးပြုချင်တဲ့အခါတွေမှာ multiple proposal ရှိနိုင်ပါတယ်။ IKEv2 proposal ကို IKEv2 policy အောက်မှာ apply လုပ်ရပါတယ်။

IKEv2 proposal ကို အသုံးပြုတဲ့အခါ သတ်မှတ်ထားတဲ့ rule တွေရှိပါတယ်။ အဲဒါတွေကတော့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

- Type တစ်ခုခြင်းစီအတွက် အနည်းဆုံး transform တစ်ခုတော့ သတ်မှတ်ပေးရပါတယ်။ ဥပမာ - Encryption method ဆိုပါတော့- အနည်းဆုံး encryption algorithm တစ်ခုတော့ သတ်မှတ်ပေးရမှာ ဖြစ်ပါတယ်။

## IKEv2

- အကယ်၍ type တစ်ခုခြင်းစီမှာ transform တစ်ခုထက်မက သတ်မှတ်ထားရင် left to right အနေနဲ့ prefer ဖြစ်ပါတယ်။
- IKEv2 initiator နဲ့ responder မှာ proposal တွေ အများကြီးရှိနေပြီး၊ တစ်ခုနဲ့တစ်ခု conflict ဖြစ်နေရင် initiator ခဲ့ proposal ကိုပဲ ဦးစားပေးမှာ ဖြစ်ပါတယ်။
- IKEv2 proposal ကို IKEv2 policy အောက်မှာ မဖြစ်မနေ reference လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ ဒါမှသာ ဘယ် proposal ကို အသုံးပြုနေတယ်ဆိုတာ သိနိုင်မှာ ဖြစ်ပါတယ်။
- IKEv2 SA negotiation အောင်မြင်ဖို့အတွက် responder မှာ initiator နဲ့ match ဖြစ်တဲ့ proposal တစ်ခုတော့ ရှိကို ရှိရပါတယ်။

### Configuring IKEv2 Proposal

```
R2(config)#crypto ikev2 proposal AMS
```

IKEv2 proposal MUST have atleast an encryption algorithm, an integrity algorithm and a dh group configured

ဒီ command ကတော့ ikev2 proposal တစ်ခုတည်ဆောက်လိုက်တာဖြစ်ပါတယ်။ proposal name ကိုသင့်တော်တဲ့ နာမည် ပေးနိုင်ပါတယ်။ အကယ်၍ လိုအပ်ရင်တော့ proposal ကို တစ်ခုထက်မကလည်း တည်ဆောက်နိုင်ပါတယ်။

```
R2(config-ikev2-proposal)#encryption aes-cbc-256 aes-cbc-192
```

ဒီ command ကတော့ encryption method သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ encryption method တစ်ခုထက်မက ပါဝင်လို့ရပါတယ်။ အခုခိုရင် aes-256 က main ဖြစ်ပြီး၊ aes-192 က backup encryption method ဖြစ်ပါတယ်။

```
R2(config-ikev2-proposal)#integrity sha512 sha256
```

ဒီ command ကတော့ integrity သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ တစ်ခုထက်မက ပါဝင်လို့ ရပါတယ်။

```
R2(config-ikev2-proposal)#group 2 5
```

## IKEv2

၃ command ကတေသ့ DH group သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ တစ်ခုထက်မက ပါဝင်လိုဂျပါတယ်။

```
R2(config-ikev2-proposal)#exit
```

```
R2(config)#crypto ikev2 policy AMSPOLICY
```

IKEv2 policy MUST have at least one complete proposal attached

၃ command ကတေသ့ IKEv2 policy တစ်ခု သတ်မှတ်ပေးလိုက်တာဖြစ်ပါတယ်။

```
R2(config-ikev2-policy)#proposal AMS
```

၃ command ကတေသ့ ရှုံးမှာ ရေးခဲ့တဲ့ proposal ကို IKEv2 policy ထဲမှာ reference လုပ်ပေးလိုက်တာဖြစ်ပါတယ်။

IKEv2 proposal တစ်ခုမှာ ပါသင့်ပါထိုက်တဲ့ အရာတွေမပါခဲ့ရင် Proposal Incomplete လို့ ပြပါလိမ့်မယ်။ ပါဝင်ရမယ့်အရာတွေကတေသ့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

```
R2 (config-ikev2-proposal) #?
```

IKEv2 Proposal commands:

<b>encryption</b>	Set encryption algorithm(s) for proposal
exit	Exit from IKEv2 proposal configuration mode
<b>group</b>	Set the Diffie-Hellman group(s)
<b>integrity</b>	Set integrity hash algorithm(s) for proposal
no	Negate a command or set its defaults
prf	Set prf algorithm(s) for proposal

```
R2 (config-ikev2-proposal) #
```

## Configuring IKEv2 Encryption

Data confidentiality အတွက် encryption algorithm ကို အသုံးပြုပါတယ်။ Cisco IOS မှာ အသုံးပြုလိုရတဲ့ encryption method တွေကတေသ့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

Algorithm	Block Size	Key Size	Strength	Quantum Resistant
AES-GCM-256	128	256	NGE	Yes
AES-GCM-128	128	128	NGE	No
AES-CBC-256	128	256	Acceptable	Yes
AES-CBC-192	128	192	Acceptable	No
AES-CBC-128	128	128	Acceptable	No
3DES	64	112	Legacy	No
DES	64	56	Avoid	No

### Configuring IKEv2 Integrity

Transit မှာ data ကို ပြုပြင်ပြောင်းလဲမှု အလုပ်မခံရပဲ မူလအတိုင်း ရှိနေအောင် ကာကွယ်ပေးဖို့အတွက် integrity algorithm ကို အသုံးပြုပါတယ်။ Cisco IOS မှာ အသုံးပြုလိုရတဲ့ integrity method တွေကတော့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

Algorithm	Checksum Size (bits)	RFC	Strength	Quantum Resistant
Sha521	256	RFC4868	NGE	Yes
Sha384	192	RFC4868	NGE	Yes
Sha256	128	RFC4868	NGE	No
Sha1	96	RFC2404	Legacy	No
Md5	96	RFC2403	Avoid	No

Initiator အနေနဲ့ Integrity ကို IKE\_SA\_INIT exchange ထဲမှာ ထည့်ပြီးပို့တာဖြစ်ပါတယ်။ proposal နဲ့ဆက်နွယ်နေတဲ့ transform တွေပါဝင်ပါတယ်။ responder အနေနဲ့ အလုပ်လုပ်နေတဲ့ device ကတော့ သူမှာ configure လုပ်ထားတဲ့ integrity algorithm ကို ရွှေးချယ်ပါတယ်။

### Configuring IKEv2 Diffie-Hellman

IPsec peer device နှစ်ခုဟာ Secure မဖြစ်တဲ့ medium ပေါ်ကနေဖြတ်ပြီး၊ shared secret တစ်ခုကို exchange လုပ်ဖို့ Diffie-Hellman group ကိုသုံးပြီး၊ Diffie-Hellman type နဲ့ size ကို ကြော်ပေးပါတယ်။ initiator အနေနဲ့ အလုပ်လုပ်နေတဲ့ device အနေနဲ့ proposal ထဲမှာ ပုစ်မခံး configure လုပ်ထားတဲ့ Diffie-Hellman public value ကို ပို့ပါတယ်။ အကယ်၍၍

## IKEv2

initiator အနေနဲ့ IKEv2 default proposal ကို အသုံးပြုမယ်ဆိုရင်တော့ Diffie-Hellman group 5 value ကို initial exchange ထဲမှာ ထည့်ပို့မှာ ဖြစ်ပါတယ်။ Cisco IOS မှာ အသုံးပြုလိုရတဲ့ Diffie-Hellman group တွေကတော့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

<b>Diffie Hellman Group</b>	<b>RFC</b>	<b>Strength</b>
1 DH 768 MODP	RFC7296	Avoid
2 DH 1024 MODP	RFC7296	Avoid
5 DH 1536 MODP	RFC7296	Avoid
14 DH 2048 MODP	RFC3526	Acceptable
15 DH 3072 MODP	RFC3526	Acceptable
16 DH 4096 MODP	RFC3526	Acceptable
19 DH 256 ECP	RFC5903	Acceptable
20 DH 384 ECP	RFC5903	NGE
21 DH 521 ECP	RFC5903	NGE
24 DH 2048 (256 subgroup) MODP	RFC5114	Acceptable

Cisco ကတော့ Group 14 or higher group တွေကို အသုံးပြုဖို့ အကြံပြုထားပါတယ်။

### Configuring IKEv2 Pseudorandom Function

Shared secret က ဆင်းသက်လာတဲ့ key material generate လုပ်ဖို့အတွက် Pseudorandom Function (PRF) ကို အသုံးပြုပါတယ်။ PRF ဆိုတာကတော့ keyed-hash message authentication code (HMAC) ကို ဆိုလိုတာ ဖြစ်ပါတယ်။ secret cryptographic key တစ်ခုနဲ့ပေါင်းစပ်ထားတဲ့ cryptographic hash function ဖြစ်ပါတယ်။ integrity algorithm ကို configure လုပ်တဲ့အခါ အဲဒီ same algorithm ကိုပဲ PRF algorithm အနေနဲ့ အသုံးပြုပါတယ်။ ဒါကြောင့် integrity configure လုပ်လိုက်တာနဲ့ PRF လည်း configure လုပ်ပြီးသား ဖြစ်ပါတယ်။ဒါပေမယ့်လည်း ဒီနေရာမှာ ထူးခြားတာတစ်ခုရှိပါတယ်။ အဲဒါကတော့ integrity algorithms MD5 and SHA1 နှစ်ခုစလုံးက 96-bit output ထွက်ပါတယ်။ ဒါပေမယ့် PRF မှာကျတော့ 96-bit output မထွက်ပဲ။ MD5 အတွက် 128-bit နဲ့ SHA1 အတွက်

## IKEv2

160-bit output ထွက်ပါတယ်။ Cisco IOS မှာ အသုံးပြုလိုရတဲ့ Pseudorandom function တွေကတော့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

Algorithm	Output Size (bits)	RFC	Strength
SHA521	256	RFC4868	NGE
SHA384	192	RFC4868	NGE
SHA256	128	RFC4868	NGE
SHA1	160	RFC2104	Legacy
MD5	128	RFC2104	Avoid

### Default IKEv2 Proposal

Default IKEv2 proposal မှာ အသုံးများတဲ့ transform value တွေပါဝင်ပါတယ်။ default IKEv2 proposal ဟာ default IKEv2 policy နဲ့လည်း associate လုပ်ပြီးသား ဖြစ်ပါတယ်။ အကယ်၍ user က သီးသန့် policy configure မလုပ်ထားရင် default policy ကို negotiate လုပ်တဲ့အခါ အသုံးပြုမှာ ဖြစ်ပါတယ်။ default policy ကို စိတ်ကြိုက်ပြင်ဆင်သလို၊ disable လည်း လုပ်နိုင်ပါတယ်။

```
R2#show crypto ikev2 proposal default
IKEv2 proposal: default
    Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
    Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
    PRF         : SHA512 SHA384 SHA256 SHA1 MD5
    DH          Group      :     DH_GROUP_1536_MODP/Group      5
    DH_GROUP_1024_MODP/Group 2
R2#
```

```
R2#show crypto ikev2 policy default
IKEv2 policy : default
    Match fvrf : any
    Match address local : any
    Proposal    : default
R2#
```

Disable လုပ်တဲ့အခါမှာလည်း default policy ကို အရင်ဖျက်ရပါတယ်။ default proposal ကို အရင်ဖျက်ရင် အသုံးပြုနေတယ်လို့ ပြပါလိမ့်မယ်။ ဖျက်ပုံးကို လေ့လာကြည့်ပါ။

## IKEv2

```
R2(config)#no crypto ikev2 proposal default
% Cannot remove as proposal is in use.
R2(config)#no crypto ikev2 policy default
R2(config)#no crypto ikev2 proposal default
R2(config)#no crypto ipsec transform-set default
```

### IKEv2 Policy

IKEv2 policy ၂ IKEv2 proposal ကို define လုပ်ပါတယ်။ IKEv2 policy မှာ အနည်းဆုံး IKEv2 proposal တစ်ခုတော့ ရှိကိုရှုပါတယ်။ optional အနေနဲ့ proposal အများကြီးလည်း ဝိုင်ပါတယ်။

#### Configuring IKEv2 Policy

##### Step 2 – IKEv2 Policy (optional)

```
R2(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R2(config-ikev2-policy)#proposal AMS-PROPOSAL
R2(config-ikev2-policy)#exit
```

```
R2(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal
attached
R2(config-ikev2-policy)#
IKEv2 Policy commands:
  exit      Exit from IKEv2 policy configuration mode
  match     Match values of local fields
  no        Negate a command or set its defaults
  proposal  Specify Proposal

R2(config-ikev2-policy)#

```

Policy scope ကို သတ်မှတ်ဖို့အတွက် match statement ကို အသုံးပြုနိုင်ပါတယ်။ IKEv2 policy ရဲအောက်မှာ match statement တစ်ခု သို့မဟုတ် တစ်ခုထက်မက အသုံးပြုလိုပါတယ်။ match statement မရှိဘူးဆိုရင်တော့ global VRF ထဲမှာ ရှိနေတဲ့ local address ကို အသုံးပြုမှာ ဖြစ်ပါတယ်။

## IKEv2

### Default IKEv2 Policy

Default IKEv2 policy မှာ default IKEv2 proposal ရှိပါတယ်။ local address အားလုံးနဲ့ match ဖြစ်ပါတယ်။ FVRF အားလုံးနဲ့လည်း match ဖြစ်ပါတယ်။ default policy ကို စိတ်ကြိုက်ပြင်နိုင်သလို၊ disable လည်း လုပ်နိုင်ပါတယ်။

### IKEv2 Keyring

IKEv2 မှာ authentication နဲ့ပက်သက်ပြီး၊ public key signatures, EAP, and shared secret ဆိုပြီး သုံးခု support လုပ်ပါတယ်။ shared secret and pre-shared key နာမည်နှစ်ခုဟာ interchangeable ဖြစ်ပါတယ်။ authentication မှာလည်း symmetric နောက် asymmetric ပါ နှစ်မျိုးလုံး support လုပ်ပါတယ်။

### Configuring IKEv2 Keyring

#### Step 3 – Crypto IKEv2 keyring (optional)

```
R2(config)#crypto ikev2 keyring AMSKEY
R2(config-ikev2-keyring)#peer R3
R2(config-ikev2-keyring-peer)#address 100.0.13.2
R2(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

### IKEv2 Profile

IKEv2 profile ကတော့ Cisco IKEv2 configuration မှာ အရေးပါဆုံးနဲ့ မဖြစ်မနေ configure လုပ်ရမှာ ဖြစ်ပါတယ်။ peer group သတ်မှတ်တာတွေ၊ parameter သတ်မှတ်တာတွေ၊ အသုံးပြုမယ့် feature တွေ သတ်မှတ်တာတွေအားလုံးက IKEv2 profile နဲ့ဆိုင်ပါတယ်။ IKEv2 profile မှာ အသုံးပြုလို့ရတဲ့ parameter နဲ့ function တွေကို အောက်မှာ လေ့လာကြည့်ပါ။

<b>IKEv2 Profile Parameter</b>	<b>Functionality Provided</b>
Match statements	Group peers based on identity
	Define scope of the profile
Authentication methods	Local and remote authentication methods
Keyring	Credentials for pre-shared key authentication method
PKI trustpoints	Credentials for certificate-based authentication methods
Local identity	Identity used by local device
AAA authorization	Authorization type, server and username
Config exchange	Configuration exchange type and behavior
Dead peer detection	DPD method and probe intervals
SA lifetime	Time-based lifetime of the IKEv2 SA
NAT keepalive	NAT keepalive duration
Initial contact	Forced initial contact processing
IVRF	IVRF of the crypto map-based IPsec Security Associations
Virtual-template	Configuration template for IPsec dVTI
Shutdown	Disable and prevent profile from being used
Redirect	Enables IKEv2 redirect feature for load balancing
Reconnect	Enables IKEv2 auto-reconnect feature

### **IKEv2 Profile Parameters and Usage**

#### **Configuring IKEv2 Profile**

```
R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate statement.
R2(config-ikev2-profile)#match identity remote address
 0.0.0.0
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#keyring local AMS_KEY
R2(config-ikev2-profile)#dpd 10 2 periodic
R2(config-ikev2-profile)#aaa authorization group psk list
  FLEX_VPN FLEX_AUTHOR
R2(config-ikev2-profile)#virtual-template 1
```

## IKEv2

```
R2 (config-ikev2-profile) #exit
```

Crypto IKEv2 profile ကို tunnel interface အောက်မှာလည်း တိုက်ရှိက် apply လုပ်နိုင်သလို၊  
IPsec profile အောက်မှာလည်း apply လုပ်နိုင်ပါတယ်။

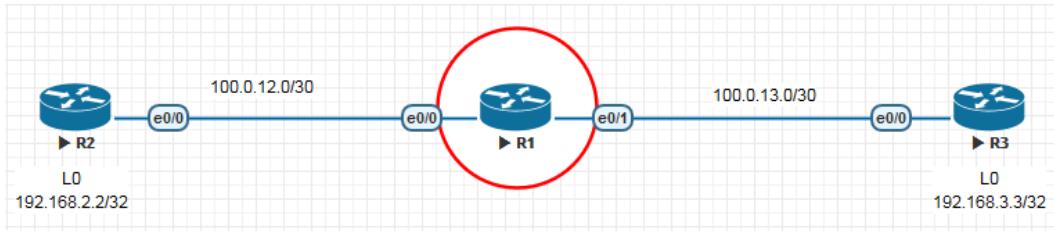
```
R2 (config-if) #tunnel protection ipsec profile AMS_IPSEC_PRO  
ikev2-profile AMS_IKEV2_PRO
```

Or

```
R2 (config) #crypto ipsec profile IPSEC_PRO  
R2 (ipsec-profile) #set transform-set AMS_SET  
R2 (ipsec-profile) #set ikev2-profile AMS_PRO  
R2 (ipsec-profile) #exit  
R2 (config-if) #tunnel protection ipsec profile AMS_IPSEC_PRO
```

## Lab – 1 Site to Site VPN with IKEv2 (IOS to IOS)

### Diagram



### Task

- Configure a LAN-to-LAN IPSec tunnel between R2 and R3. You must use the following attributes for phase 1 and phase 2 negotiation:

#### Phase 1 setting (IKEv2):

1. Use AES-CBS-256 for encryption and backup as AES-CBS-192.
2. Use SHA-512 for integrity and backup as SHA-256.
3. Use DH group 2 and backup as group 5.
4. Use Pre-Shared key AMSCISCO for authentication.

#### Phase 2 setting (IPsec)

1. Use AES 128 and SHA-1 for traffic encryption and integrity validation respectively.
2. Only protect traffic between 192.168.2.2/32 and 192.168.3.3/32

### Solution

#### ISP

```

ISP(config)#interface Ethernet0/0
ISP(config-if)# ip address 100.0.12.1 255.255.255.252
ISP(config-if)#no shut
ISP(config)#interface Ethernet0/1
ISP(config-if)# ip address 100.0.13.1 255.255.255.252
ISP(config-if)#no shut
  
```

## IKEv2

R2

```
R2(config)#interface Ethernet0/0
R2(config-if)# ip address 100.0.12.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1

R2(config)#crypto ikev2 proposal AMS
IKEv2 proposal MUST have atleast an encryption algorithm,
an integrity algorithm and a dh group configured

R2(config-ikev2-proposal)#encryption aes-cbc-256 aes-cbc-192
R2(config-ikev2-proposal)#integrity sha512 sha256
R2(config-ikev2-proposal)#group 2 5
R2(config-ikev2-proposal)#exit

R2(config)#crypto ikev2 policy AMSPOLICY
IKEv2 policy MUST have atleast one complete proposal attached
R2(config-ikev2-policy)#proposal AMS

R2(config)#crypto ikev2 keyring AMSKEY
R2(config-ikev2-keyring)#peer R3
R2(config-ikev2-keyring-peer)#address 100.0.13.2
R2(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
OR
For asymmetric key
R2(config-ikev2-keyring-peer)#pre-shared-key local R2AMSCISCO
R2(config-ikev2-keyring-peer)#pre-shared-key remote R3AMSCISCO
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit

R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
1. A local and a remote authentication method.
2. A match identity or a match certificate statement.
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#match identity remote address 100.0.13.2
R2(config-ikev2-profile)#keyring local AMSKEY
R2(config-ikev2-profile)#exit
```

## IKEv2

```
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#exit

R2(config)#ip access-list extended R2_TO_R3
R2(config-ext-nacl)#permit ip host 192.168.2.2 host
192.168.3.3
R2(config-ext-nacl)#exit

R2(config)#crypto map VPN_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
and a valid access list have been configured.
R2(config-crypto-map)#set peer 100.0.13.2
R2(config-crypto-map)#set transform-set AMS_SET
R2(config-crypto-map)#mat address R2_TO_R3
R2(config-crypto-map)#set ikev2-profile AMS_PRO

R2(config)#interface Ethernet0/0
R2(config-if)#crypto map VPN_MAP
```

## R3

```
R3(config)#interface Ethernet0/0
R3(config-if)# ip address 100.0.13.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1

R3(config)#crypto ikev2 proposal AMS
IKEv2 proposal MUST have atleast an encryption algorithm,
an integrity algorithm and a dh group configured

R3(config-ikev2-proposal)#encryption aes-cbc-256 aes-cbc-
192
R3(config-ikev2-proposal)#integrity sha512 sha256
R3(config-ikev2-proposal)#group 2 5
R3(config-ikev2-proposal)#exit

R3(config)#crypto ikev2 policy AMSPOLICY
IKEv2 policy MUST have atleast one complete proposal attached
R3(config-ikev2-policy)#proposal AMS

R3(config)#crypto ikev2 keyring AMSKEY
```

## IKEv2

```
R3(config-ikev2-keyring)#peer R2
R3(config-ikev2-keyring-peer)#address 100.0.12.2
R3(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
OR
For asymmetric key
R3(config-ikev2-keyring-peer)#pre-shared-key local
R3AMSCISCO
R3(config-ikev2-keyring-peer)#pre-shared-key remote
R2AMSCISCO
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit

R3(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
  1. A local and a remote authentication method.
  2. A match identity or a match certificate statement.
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#match identity remote address
100.0.12.2
R3(config-ikev2-profile)#keyring local AMSKEY
R3(config-ikev2-profile)#exit

R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R3(crypto-trans)#exit

R3(config)#ip access-list extended R3_TO_R2
R3(config-ext-nacl)#permit ip host 192.168.3.3 host
192.168.2.2
R3(config-ext-nacl)#exit

R3(config)#crypto map VPN_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
          and a valid access list have been configured.
R3(config-crypto-map)#set peer 100.0.12.2
R3(config-crypto-map)#set transform-set AMS_SET
R3(config-crypto-map)#mat address R3_TO_R2
R3(config-crypto-map)#set ikev2-profile AMS_PRO

R3(config)#interface Ethernet0/0
R3(config-if)#crypto map VPN_MAP
```

### Verification

```
R2#ping 192.168.3.3 so 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
R2#
```

```
R2#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id Local           Remote           fvrf/ivrf      Status
1       100.0.12.2/500     100.0.13.2/500   none/none      READY
SK      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:2, Auth sign: PSK, Auth ve
          Life/Active Time: 86400/1471 sec

IPv6 Crypto IKEv2 SA

R2#
```

```
R2#show crypto ikev2 session
IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local           Remote           fvrf/ivrf      Status
1       100.0.12.2/500     100.0.13.2/500   none/none      READY
SK      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:2, Auth sign: PSK, Auth v
          Life/Active Time: 86400/1548 sec
Child sa: local selector 192.168.2.2/0 - 192.168.2.2/65535
          remote selector 192.168.3.3/0 - 192.168.3.3/65535
          ESP spi in/out: 0x6C333BE1/0xAC89E4D9

IPv6 Crypto IKEv2 Session

R2#
```

Phase 1 ကိစစ်ကြည့်လိုက်တဲ့အခါ အောင်မြင်နေပါပြီ။ phase 1 ကိစစ်ပို့ show crypto ikev2 sa နဲ့ show crypto ikev2 session တို့ကိုသုံးနိုင်ပါတယ်။ Phase 2 ကို ဆက်စစ်ကြည့်ပါမယ်။

R2#show crypto ipsec sa

```
interface: Ethernet0/0
  Crypto map tag: VPN_MAP, local addr 100.0.12.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.3/255.255.255.255/0/0)
  current_peer 100.0.13.2 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

## Explanation

### IKEv2 Proposal

IKEv2 proposal ကတေသာ cryptographic transform ကို သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ IKEv2 proposal မှာ configure လုပ်ထားတဲ့ transform type တွေကတေသာ encryption algorithm, pseudorandom function, integrity algorithm နဲ့ Diffie-Hellman group ဖြစ်ပါတယ်။ IKEv1 နဲ့ မတူတာတစ်ခုကတေသာ authentication method နဲ့ SA lifetime ကို negotiate မလုပ်ပါဘူး။ ဒါကြောင့် proposal ထဲမှာ authentication method နဲ့ SA lifetime မပါဝင်ပါဘူး။

IKE V1	IKE V2
1)IKEv1 policy	1a) IKev2 proposal
2)Keying	1b) IKev2 policy
3)IPsec	2a) keying
4)interesting ACL	2b)IKev2 profile
5)Crypto map	3)IPsec
6)Apply to interface	4) ACL
	5) crypto map
	6) apply to interface

#### R2(config)#**crypto ikev2 proposal AMS**

IKEv2 proposal MUST have at least an encryption algorithm, an integrity algorithm and a dh group configured

ဒါ command ကတေသာ ikev2 proposal တစ်ခုတည်ဆောက်လိုက်တာဖြစ်ပါတယ်။ proposal name ကိုသင့်တော်တဲ့ နာမည် ပေးနိုင်ပါတယ်။ အကယ်၍ လိုအပ်ရင်တော့ proposal ကို တစ်ခုထောက်မကလည်း တည်ဆောက်နိုင်ပါတယ်။

R2(config-ikev2-proposal)#**encryption aes-cbc-256 aes-cbc-192**

## IKEv2

၃ command ကတေသ့ encryption method သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ encryption method တစ်ခုထက်မက ပါဝင်လို့ရပါတယ်။ အခုဆိုရင် aes-256 က main ဖြစ်ပြီး၊ aes-192 က backup encryption method ဖြစ်ပါတယ်။

R2(config-ikev2-proposal)#**integrity sha512 sha256**

၃ command ကတေသ့ integrity သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ တစ်ခုထက်မက ပါဝင်လို့ရပါတယ်။

R2(config-ikev2-proposal)#**group 2 5**

R2(config-ikev2-proposal)#exit

၃ command ကတေသ့ DH group သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ တစ်ခုထက်မက ပါဝင်လို့ရပါတယ်။

R2(config)#**crypto ikev2 policy AMSPOLICY**

IKEv2 policy MUST have atleast one complete proposal attached

၃ command ကတေသ့ IKEv2 policy တစ်ခု သတ်မှတ်ပေးလိုက်တာဖြစ်ပါတယ်။

R2(config-ikev2-policy)#**proposal AMS**

၃ command ကတေသ့ ရွှေ့မှာ ရေးခဲ့တဲ့ proposal ကို IKEv2 policy ထဲမှာ reference လုပ်ပေးလိုက်တာဖြစ်ပါတယ်။

R2(config)#**crypto ikev2 keyring AMSKEY**

၃ command ကတေသ့ IKEv2 keyring name သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ သင့်တော်တဲ့ နာမည် ပေးနိုင်ပါတယ်။

R2(config-ikev2-keyring)#**peer R3**

၃ command ကတေသ့ peer ကို သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ သင့်တော်တဲ့ နာမည်ပေးနိုင်ပါတယ်။

R2(config-ikev2-keyring-peer)#**address 100.0.13.2**

၃ command ကတေသ့ remote peer ရဲ့ address ကို သတ်မှတ်ပေးတာဖြစ်ပါတယ်။

R2(config-ikev2-keyring-peer)#**pre-shared-key AMSCISCO**

## IKEv2

၃ command ကတေသ့ preshared key ကိုသတ်မှတ်ပေးတာဖြစ်ပါတယ်။ အကယ်၍ နှစ်ဘက် key မတူအောင် ထားချွင်ရင်တေ့ အောက်ပါအတိုင်း configure လုပ်နိုင်ပါတယ်။

OR

For asymmetric key

```
R2(config-ikev2-keyring-peer)#pre-shared-key local R2AMSCISCO
```

```
R2(config-ikev2-keyring-peer)#pre-shared-key remote R3AMSCISCO
```

```
R2(config-ikev2-keyring-peer)#exit
```

```
R2(config-ikev2-keyring)#exit
```

**R2(config)#crypto ikev2 profile AMS\_PRO**

IKEv2 profile MUST have:

1. A local and a remote authentication method.
2. A match identity or a match certificate statement.

၃ command ကတေသ့ IKEv2 profile ဆောက်ပေးတာဖြစ်ပါတယ်။

```
R2(config-ikev2-profile)#authentication local pre-share
```

၃ command ကတေသ့ authentication ကို pre-share key ကိုသုံးမယ်လို့ ပြောတာဖြစ်ပါတယ်။

```
R2(config-ikev2-profile)#authentication remote pre-share
```

၃ command ကတေသ့ remote peer အတွက်လည်း authentication pre-share ကိုသုံးမယ်လို့ပြောတာဖြစ်ပါတယ်။

```
R2(config-ikev2-profile)#match identity remote address 100.0.13.2
```

၃ command ကတေသ့ remote address ကို သတ်မှတ်ပေးတာဖြစ်ပါတယ်။

```
R2(config-ikev2-profile)#keyring local AMSKEY
```

၃ command ကတေသ့ ရှေ့မှာ configure လုပ်ခဲ့တဲ့ key ကို ပြန်ပြီး reference လုပ်ပေးလိုက်တာဖြစ်ပါတယ်။

```
R2(config-ikev2-profile)#exit
```

**R2(config)#crypto ipsec transform-set AMS\_SET esp-aes esp-sha-hmac**

## IKEv2

```
R2(cfg-crypto-trans)#exit
```

ဦး command ကတေသ့ transform-set တည်ဆောက်ပြီး phase 2 အတွက် encryption method နဲ့ authentication method ကိုသတ်မှတ်ပေးတာဖြစ်ပါတယ်။

```
R2(config)#ip access-list extended R2_TO_R3
```

```
R2(config-ext-nacl)#permit ip host 192.168.2.2 host 192.168.3.3
```

```
R2(config-ext-nacl)#exit
```

ဦး command ကတေသ့ IPsec VPN tunnel ထဲကနေ သွားခွင့်ပေးမယ့် interesting traffic ကို သတ်မှတ်ပေးတာဖြစ်ပါတယ်။

```
R2(config)#crypto map VPN_MAP 10 ipsec-isakmp
```

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

ဦး command ကတေသ့ crypto map တစ်ခု တည်ဆောက်ပေးတာဖြစ်ပါတယ်။

```
R2(config-crypto-map)#set peer 100.0.13.2
```

```
R2(config-crypto-map)#set transform-set AMS_SET
```

```
R2(config-crypto-map)#map address R2_TO_R3
```

```
R2(config-crypto-map)#set ikev2-profile AMS_PRO
```

ဦး command တွေကတော့ ရှေ့မှာ ရေးခဲ့တဲ့ ACL, IKEv2 profile , transform set တွေနဲ့ peer IP ကို ပြန်ထည့်ပေးတာဖြစ်ပါတယ်။

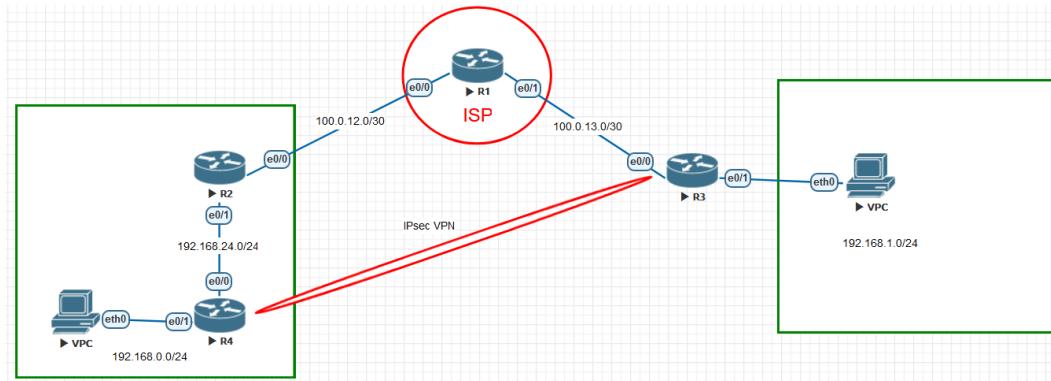
```
R2(config)#interface Ethernet0/0
```

```
R2(config-if)#crypto map VPN_MAP
```

ဦး command ကတေသ့ crypto map ကို interface အောက်မှာ apply လုပ်လိုက်တာဖြစ်ပါတယ်။

## Lab – 2 Site to Site VPN with IKE v2 with NAT-T (IOS to IOS)

### Diagram



### Task

- Configure a LAN-to-LAN IPSec tunnel between R3 and R4. You must use the following attributes for phase 1 and phase 2 negotiation:

#### Phase 1 setting (IKEv2):

1. Use AES-CBS-256 for encryption and backup as AES-CBS-192.
2. Use SHA-512 for integrity and backup as SHA-256.
3. Use DH group 2 and backup as group 5.
4. Use Pre-Shared key AMSCISCO for authentication.

#### Phase 2 setting (IPsec)

1. Use AES 128 and SHA-1 for traffic encryption and integrity validation respectively.
2. Only protect traffic between 192.168.0.0/24 and 192.168.1.0/24

### Solution

#### ISP

```

ISP(config)#interface Ethernet0/0
ISP(config-if)# ip address 100.0.12.1 255.255.255.252
ISP(config-if)#no shut
ISP(config)#interface Ethernet0/1
ISP(config-if)# ip address 100.0.13.1 255.255.255.252
ISP(config-if)#no shut

```

## IKEv2

### R2

```
R2(config)#interface Ethernet0/0
R2(config-if)# ip address 100.0.12.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface Ethernet0/1
R2(config-if)# ip address 192.168.24.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit

R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1
```

### R4

```
R4(config)#interface Ethernet0/0
R4(config-if)# ip address 192.168.24.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#interface Ethernet0/1
R4(config-if)# ip address 192.168.0.1 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit

R4(config)#ip route 0.0.0.0 0.0.0.0 192.168.24.2

R4(config)#crypto ikev2 proposal AMS
IKEv2 proposal MUST have atleast an encryption algorithm,
an integrity algorithm and a dh group configured

R4(config-ikev2-proposal)#encryption aes-cbc-256 aes-cbc-192
R4(config-ikev2-proposal)#integrity sha512 sha256
R4(config-ikev2-proposal)#group 2 5
R4(config-ikev2-proposal)#exit

R4(config)#crypto ikev2 policy AMSPOLICY
IKEv2 policy MUST have atleast one complete proposal
attached
R4(config-ikev2-policy)#proposal AMS

R4(config)#crypto ikev2 keyring AMSKEY
R4(config-ikev2-keyring)#peer R3
R4(config-ikev2-keyring-peer)#address 0.0.0.0
R4(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
OR
```

## IKEv2

```

For asymmetric key
R4(config-ikev2-keyring-peer) #pre-shared-key local
R4AMSCISCO
R4(config-ikev2-keyring-peer) #pre-shared-key remote
R3AMSCISCO
R4(config-ikev2-keyring-peer) #exit
R4(config-ikev2-keyring) #exit

R4(config) #crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate statement.
R4(config-ikev2-profile) #authentication local pre-share
R4(config-ikev2-profile) #authentication remote pre-share
R4(config-ikev2-profile) #match identity remote address
0.0.0.0
R4(config-ikev2-profile) #keyring local AMSKEY
R4(config-ikev2-profile) #exit

R4(config) #crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R4(cfg-crypto-trans) #exit

R4(config) #ip access-list extended R4_TO_R3
R4(config-ext-nacl) #permit ip 192.168.0.0 0.0.0.255
192.168.1.0 0.0.0.255
R4(config-ext-nacl) #exit

R4(config) #crypto map VPN_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R4(config-crypto-map) #set peer 100.0.13.2
R4(config-crypto-map) #set transform-set AMS_SET
R4(config-crypto-map) #mat address R4_TO_R3
R4(config-crypto-map) #set ikev2-profile AMS_PRO

R4(config) #interface Ethernet0/0
R4(config-if) #crypto map VPN_MAP

```

## R3

```

R3(config) #interface Ethernet0/0
R3(config-if) # ip address 100.0.13.2 255.255.255.252
R3(config-if) #no shut

```

## IKEv2

```
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1

R3(config)#crypto ikev2 proposal AMS
IKEv2 proposal MUST have atleast an encryption algorithm,
an integrity algorithm and a dh group configured

R3(config-ikev2-proposal)#encryption aes-cbc-256 aes-cbc-192
R3(config-ikev2-proposal)#integrity sha512 sha256
R3(config-ikev2-proposal)#group 2 5
R3(config-ikev2-proposal)#exit

R3(config)#crypto ikev2 policy AMSPOLICY
IKEv2 policy MUST have atleast one complete proposal
attached
R3(config-ikev2-policy)#proposal AMS

R3(config)#crypto ikev2 keyring AMSKEY
R3(config-ikev2-keyring)#peer R4
R3(config-ikev2-keyring-peer)#address 0.0.0.0
R3(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
OR
For asymmetric key
R3(config-ikev2-keyring-peer)#pre-shared-key local
R3AMSCISCO
R3(config-ikev2-keyring-peer)#pre-shared-key remote
R4AMSCISCO
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit

R3(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate statement.
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#match identity remote address
0.0.0.0
R3(config-ikev2-profile)#keyring local AMSKEY
R3(config-ikev2-profile)#exit

R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R3(cfg-crypto-trans)#exit
```

## IKEv2

```
R3(config)#ip access-list extended R3_TO_R4
R3(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255
192.168.0.0 0.0.0.255
R3(config-ext-nacl)#exit

R3(config)#crypto map VPN_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
and a valid access list have been configured.
R3(config-crypto-map)#set peer 100.0.12.2
R3(config-crypto-map)#set transform-set AMS_SET
R3(config-crypto-map)#mat address R3_TO_R4
R3(config-crypto-map)#set ikev2-profile AMS_PRO

R3(config)#interface Ethernet0/0
R3(config-if)#crypto map VPN_MAP
```

## Verification

```
R4#ping 192.168.1.1 source 192.168.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/14 ms
R4#
```

```
R4#show crypto session
Crypto session current status

Interface: Ethernet0/0
Profile: AMS_PRO
Session status: UP-ACTIVE
Peer: 100.0.13.2 port 4500
Session ID: 1
IKEv2 SA: local 192.168.24.4/4500 remote 100.0.13.2/4500
Active
IPSEC FLOW: permit ip 192.168.0.0/255.255.255.0
192.168.1.0/255.255.255.0
Active SAs: 2, origin: crypto map

R4#
```

## IKEv2

```
R4#show crypto ikev2 sa
IPv4 Crypto IKEV2 SA
Tunnel-id Local           Remote           fvrf/ivrf          Status
1      192.168.24.4/4500   100.0.13.2/4500   none/none          READY
    Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:2, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/149 sec
```

IPv6 Crypto IKEV2 SA

R4#

```
R4#show crypto ikev2 session
IPv4 Crypto IKEV2 Session
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local           Remote           fvrf/ivrf          Status
1      192.168.24.4/4500   100.0.13.2/4500   none/none          READY
    Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:2, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/222 sec
Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535
          remote selector 192.168.1.0/0 - 192.168.1.255/65535
          ESP spi in/out: 0x120B3393/0x1BF780D3
IPv6 Crypto IKEV2 Session
R4#
```

Phase 1 ကိစစ်ကြည့်လိုက်တဲ့အခါ အောင်မြင်နေပါပြီ။ phase 1 ကိစစ်ဖို့ show crypto ikev2 sa နဲ့ show crypto ikev2 session တို့ကိုသုတေသနပါတယ်။

Phase 2 ကို ဆက်စစ်ကြည့်ပါမယ်။

```
R4#show crypto ipsec sa

interface: Ethernet0/0
Crypto map tag: VPN_MAP, local addr 192.168.24.4

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 100.0.13.2 port 4500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
```

## Explanation

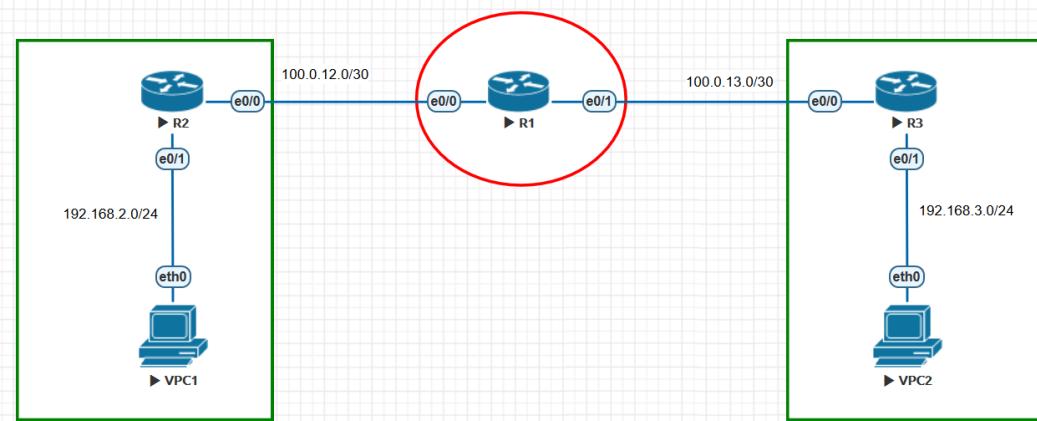
Site to site VPN with IKEv2 lab နဲ့ အတူတူပဲ ဖြစ်ပါတယ်။ ကွာခြားချက်ကတော့ IPsec VPN tunnel တည်ဆောက်မယ့် R4 ဟာ NAT device ဖြစ်တဲ့ R2 နောက်မှာ ရှိနေတာပဲ ဖြစ်ပါတယ်။ ဒီနေရာမှာ သတိထားရမယ့်အချက်ကတော့ **keyring** နဲ့ **IKEv2 profile configure** လုပ်တဲ့ အခါမှာတော့ **address** ကို 0.0.0.0 ထားပေးရမှာ ဖြစ်ပါတယ်။ SVTI မှာလည်း ဒီအတိုင်းပဲ

## IKEv2

ဖြစ်ပါတယ်။ နောက်တစ်ချက်ကတော့ R4 က စုံပြီး initiate လုပ်မယ်ဆိုရင်တော့ R2 မှ port 4500 အတွက် static NAT ရေးပေးစရာမလိုပါဘူး။ ဘာကြောင့်လဲဆိုတော့ အခုအသုံးပြုနေတဲ့ IOS version က 15.4 ဖြစ်ပါတယ်။

### Lab – 3 Site to Site VPN with IKE v2 with Dynamic IP

#### Diagram



#### Task

Configure IKEv2 Site-to-Site VPN using the following parameter:

IKEv2 Proposal	
Encryption	aes-cbc-256
Integrity	sha256
Group	group 14

IKEv2 Policy	
Match fvrf	global
Match address local	any
Proposal	AMS-PROPOSAL

## IKEv2

IKEv2 Keyring	
Peer	R2 and R3
address	100.0.12.2 and dynamic IP
pre-shared-key	AMSCISCO

IKEv2 Profile	
Profile Name	AMS_PRO
address	100.0.12.2 and dynamic IP
Authentication	Pre-share

Crypto ACL and Transform -set	
Transform-set name	AMS_SET
Encryption and Authenticaiton	esp-aes 256 esp-sha-hmac
Crypto ACL	192.168.2.0/24 and 192.168.3.0/24

## Solution

Step 1 – IKEv2 Proposal (optional)

Step 2 – IKEv2 Policy (optional)

Step 3 – Crypto IKEv2 keyring (optional)

Step 4 – Crypto IKEv2 profile

Step 5 – Crypto ACL and IPsec Transform Set

Step 6 – Crypto Map

### Step 1 – IKEv2 Proposal (optional)

Step 1 – IKEv2 Proposal (optional)

```
R2(config)#crypto ikev2 proposal AMS-PROPOSAL
R2(config-ikev2-proposal)#encryption aes-cbc-256
R2(config-ikev2-proposal)#integrity sha256
R2(config-ikev2-proposal)#group 14
R2(config-ikev2-proposal)#exit
```

## IKEv2

---

### Step 2 – IKEv2 Policy (optional)

#### Step 2 – IKEv2 Policy (optional)

```
R2(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R2(config-ikev2-policy)#proposal AMS-PROPOSAL
R2(config-ikev2-policy)#exit
```

### Step 3 – Crypto IKEv2 keyring (optional)

#### Step 3 – Crypto IKEv2 keyring (optional)

```
R2(config)#crypto ikev2 keyring AMSKEY
R2(config-ikev2-keyring)#peer R3
R2(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0
R2(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

### Step 4 – Crypto IKEv2 profile

#### Step 4 – Crypto IKEv2 profile

```
R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any statement.
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#match identity remote address 0.0.0.0
R2(config-ikev2-profile)#keyring local AMSKEY
R2(config-ikev2-profile)#exit
```

### Step 5 – Crypto ACL and IPsec Transform Set

#### Step 5 – Crypto ACL and IPsec Transform Set

```
R2(config)#ip access-list extended R2_TO_R3
R2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
R2(config-ext-nacl)#exit

R2(config)#crypto ipsec transform-set AMS_SET esp-aes 256
esp-sha-hmac
R2(cfg-crypto-trans)#exit
```

## IKEv2

### Step 6 – Crypto map

#### Step 6 – Crypto map

```
R2(config)#crypto dynamic-map AMS_MAP 10
R2(config-crypto-map)#set transform-set AMS_SET
R2(config-crypto-map)#set ikev2-profile AMS_PRO
R2(config-crypto-map)#match address R2_TO_R3
R2(config-crypto-map)#exit

R2(config)#crypto map VPN_MAP 1 ipsec-isakmp dynamic
AMS_MAP
R2(config)#interface ethernet 0/0
R2(config-if)#crypto map VPN_MAP
R2(config-if)#exit
```

#### Step 1 – IKEv2 Proposal (optional)

```
R3(config)#crypto ikev2 proposal AMS-PROPOSAL
R3(config-ikev2-proposal)#encryption aes-cbc-256
R3(config-ikev2-proposal)#integrity sha256
R3(config-ikev2-proposal)#group 14
R3(config-ikev2-proposal)#exit
```

#### Step 2 – IKEv2 Policy (optional)

```
R3(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R3(config-ikev2-policy)#proposal AMS-PROPOSAL
R3(config-ikev2-policy)#exit
```

#### Step 3 – Crypto IKEv2 keyring (optional)

```
R3(config)#crypto ikev2 keyring AMSKEY
R3(config-ikev2-keyring)#peer R2
R3(config-ikev2-keyring-peer)#address 100.0.12.2
R3(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit
```

#### Step 4 – Crypto IKEv2 profile

```
R3(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any statement.
```

## IKEv2

```
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#match identity remote address 100.0.12.2
R3(config-ikev2-profile)#keyring local AMSKEY
R3(config-ikev2-profile)#exit
```

### Step 5 – Crypto ACL and IPsec Transform Set

```
R3(config)#ip access-list extended R3_TO_R2
R3(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
R3(config-ext-nacl)#exit

R3(config)#crypto ipsec transform-set AMS_SET esp-aes 256
esp-sha-hmac
R3(cfg-crypto-trans)#exit
```

### Step 6 – Crypto map

```
R3(config)#crypto map AMS_MAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
R3(config-crypto-map)#set peer 100.0.12.2
R3(config-crypto-map)#set transform-set AMS_SET
R3(config-crypto-map)#set ikev2-profile AMS_PRO
R3(config-crypto-map)#match address R3_TO_R2
R3(config-crypto-map)#exit

R3(config)#interface ethernet 0/0
R3(config-if)#crypto map AMS_MAP
R3(config-if)#exit
*Aug 22 16:53:47.823: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

## Verification

```
R2#ping 192.168.3.1 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms
R2#
```

## IKEv2

```
R2#show crypto engine connections active
Crypto Engine Connections

  ID  Type    Algorithm          Encrypt  Decrypt  LastSeqN IP-Address
  3   IPsec   AES256+SHA        5         0        0 100.0.12.2
  4   IPsec   AES256+SHA        0         5        5 100.0.12.2
1001  IKEv2  SHA256+AES256     0         0        0 100.0.12.2

R2#
```

```
R2#show crypto ikev2 session
  IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

  Tunnel-id Local                  Remote                  fvrif/ivrf
  Status
  1           100.0.12.2/500       100.0.13.2/500       none/none
  READY
    Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14,
    Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/3869 sec
  Child sa: local selector 192.168.2.0/0 - 192.168.2.255/65535
            remote selector 192.168.3.0/0 - 192.168.3.255/65535
            ESP spi in/out: 0x90A08075/0x626051D5

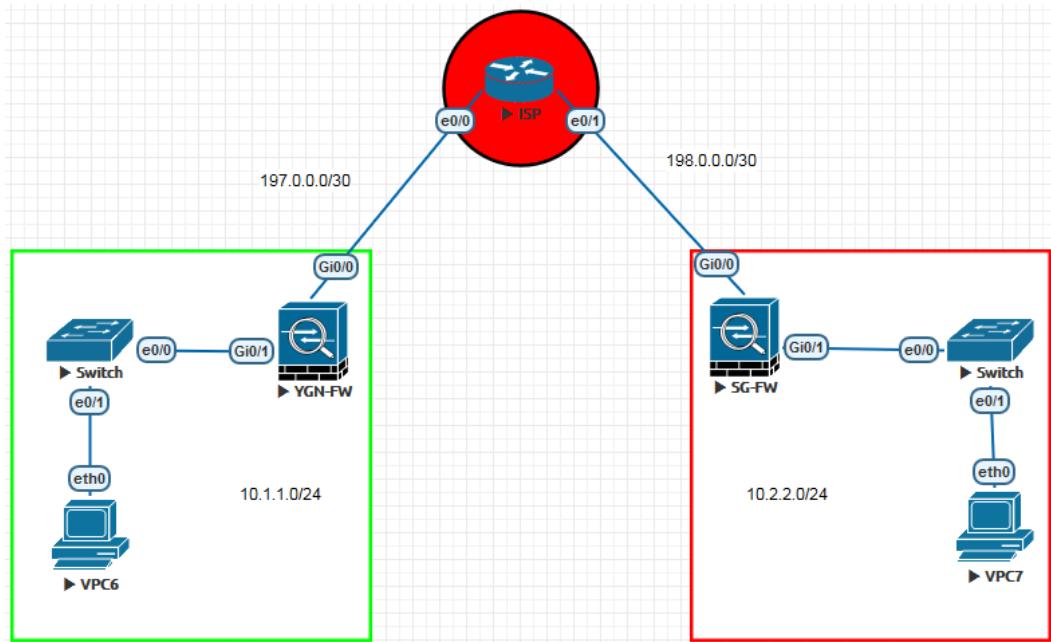
  IPv6 Crypto IKEv2 Session

R2#
```

Dynamic IP address အသံးပြုနေတဲ့ peer ဘက်ကစွမ်း traffic ကို ပြုလုပ်တယ်။

## Lab – 4 Site to Site VPN using IKEv2 on ASA 9.7

### Diagram



### Task

- Configure IPsec site to site VPN on ASA using IKEv2.

### Configuration Steps on ASA

9. Enable ISAKMP.
10. Create ISAKMP policy.
11. Set the tunnel type.
12. Define the IPsec policy.
13. Configure the crypto map.
14. Configure traffic filtering (optional).
15. Bypass NAT (optional)
16. Enable Perfect Forward Secrecy (optional).

## Solution

YGN

```

ciscoasa(config)# hostname YGN
YGN(config)# interface gi0/0
YGN(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
YGN(config-if)# ip address 197.0.0.2 255.255.255.252
YGN(config-if)# no shutdown
YGN(config-if)# interface gi0/1
YGN(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
YGN(config-if)# ip address 10.1.1.1 255.255.255.0
YGN(config-if)# no shutdown
YGN(config-if)# exit
YGN(config)# route outside 0.0.0.0 0.0.0.0 197.0.0.1

YGN(config)# crypto ikev2 enable outside
YGN(config)# crypto ikev2 policy 1
YGN(config-ikev2-policy)# encryption 3des
YGN(config-ikev2-policy)# integrity sha
YGN(config-ikev2-policy)# group 5
YGN(config-ikev2-policy)# prf sha

YGN(config)# tunnel-group 198.0.0.2 type ipsec-l2l
YGN(config)# tunnel-group 198.0.0.2 ipsec-attributes
YGN(config-tunnel-ipsec)# ikev2 remote-authentication pre-
shared-key AMS@VPN
YGN(config-tunnel-ipsec)# ikev2 local-authentication pre-
shared-key AMS@VPN

YGN(config)#crypto ipsec ikev2 ipsec-proposal YGN_TO_SG
YGN(config-ipsec-proposal)# protocol esp encryption aes-
256
YGN(config-ipsec-proposal)# protocol esp integrity sha-512

YGN(config)# access-list YGN_TO_SG line 1 remark To
encrypt from YGN to SG
YGN(config)# access-list YGN_TO_SG line 2 extended permit
ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

YGN(config)# crypto map YGN_MAP 1 match address
YGN_TO_SG
YGN(config)# crypto map YGN_MAP 1 set peer 198.0.0.2

```

## IKEv2

```
YGN(config)# crypto map YGN_MAP 1 set ikev2 ipsec-
proposal YGN_TO_SG
YGN(config)# crypto map YGN_MAP interface outside
```

SG

```
SG(config)# interface gi0/0
SG(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
SG(config-if)# ip address 198.0.0.2 255.255.255.252
SG(config-if)# no shutdown
SG(config-if)# interface gi0/1
SG(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
SG(config-if)# ip address 10.2.2.1 255.255.255.0
SG(config-if)# no shutdown
SG(config-if)# exit
SG(config)# route outside 0.0.0.0 0.0.0.0 198.0.0.1

SG(config)#crypto ikev2 enable outside
SG(config)#crypto ikev2 policy 1
SG(config-ikev2-policy)# encryption 3des
SG(config-ikev2-policy)#integrity sha
SG(config-ikev2-policy)#group 5
SG(config-ikev2-policy)#prf sha

SG(config)# tunnel-group 197.0.0.2 type ipsec-l2l
SG(config)# tunnel-group 197.0.0.2 ipsec-attributes
SG(config-tunnel-ipsec)# ikev2 remote-authentication pre-
shared-key AMS@VPN
SG(config-tunnel-ipsec)# ikev2 local-authentication pre-
shared-key AMS@VPN

SG(config)# crypto ipsec ikev2 ipsec-proposal SG_TO_YGN
SG(config-ipsec-proposal)# protocol esp encryption aes-256
SG(config-ipsec-proposal)# protocol esp integrity sha-512

SG(config)# access-list SG_TO_YGN line 1 remark To
encrypt from YGN to SG
SG(config)# access-list SG_TO_YGN line 2 extended permit
ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0

SG(config)# crypto map SG_MAP 1 match address SG_TO_YGN
SG(config)# crypto map SG_MAP 1 set peer 197.0.0.2
SG(config)# crypto map SG_MAP 1 set ikev2 ipsec-proposal
SG_TO_YGN
```

## IKEv2

```
SG(config)# crypto map SG_MAP interface outside
```

### Verification

YGN-PC> ping 10.2.2.10

```
84 bytes from 10.2.2.10 icmp_seq=1 ttl=64 time=7.447 ms
84 bytes from 10.2.2.10 icmp_seq=2 ttl=64 time=6.131 ms
84 bytes from 10.2.2.10 icmp_seq=3 ttl=64 time=12.289 ms
84 bytes from 10.2.2.10 icmp_seq=4 ttl=64 time=5.367 ms
84 bytes from 10.2.2.10 icmp_seq=5 ttl=64 time=8.495 ms
```

YGN-PC>

YGN# show crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	Status	Role
73089419	197.0.0.2/500	198.0.0.2/500	READY	INITIATOR
	Encr: 3DES, Hash: SHA96, DH Grp:5, Auth sign: PSK, Auth verify: PSK			
	Life/Active Time: 86400/209 sec			
Child sa:	local selector 10.1.1.0/0 - 10.1.1.255/65535			
	remote selector 10.2.2.0/0 - 10.2.2.255/65535			
	ESP spi in/out: 0x15594df7/0x1b029862			

YGN#

```
YGN# sh crypto ipsec sa
interface: outside
    Crypto map tag: YGN_MAP, seq num: 1, local addr:
    197.0.0.2

        access-list YGN_TO_SG extended permit ip 10.1.1.0
        255.255.255.0 10.2.2.0 255.255.255.0
            local ident (addr/mask/prot/port):
            (10.1.1.0/255.255.255.0/0/0)
            remote ident (addr/mask/prot/port):
            (10.2.2.0/255.255.255.0/0/0)
            current_peer: 198.0.0.2

            #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
            #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
            #pkts compressed: 0, #pkts decompressed: 0
            #pkts not compressed: 4, #pkts comp failed: 0, #pkts
```

### Useful show command

- debug crypto ikev2 platform 5 - debug phase 1 (ISAKMP SA's)
- debug crypto ikev2 protocol 5 - debug phase 1 (ISAKMP SA's)

## IKEv2

- debug crypto ipsec - debug phase 2 (IPSEC SA's)
- show crypto ikev2 sa - show phase 1 SA's
- show crypto ipsec sa - show phase 2 SA's

### Explanation

IKEv1 နဲ့ ယူဉ်လိုက်ရင် IKEv2 မှာ ကောင်းတဲ့ အချက်ထွေကတွေ asymmetric authentication method သုံးလို့ရတာတွေ၊ IKE DoS attack ကို protection လုပ်တဲ့ အခါ ပိုကောင်းလာတာတွေ၊ SA establishment လုပ်တဲ့ အခါ message overhead မဖြစ်ခြင်း စတာတွေဖြစ်ပါတယ်။

### Encryption Domain

```
access-list YGN_TO_SG remark To encrypt from YGN to SG
access-list YGN_TO_SG extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0
255.255.255.0

access-list SG_TO_YGN remark To encrypt from YGN to SG
access-list SG_TO_YGN extended permit ip 10.2.2.0 255.255.255.0 10.1.1.0
255.255.255.0
```

Tunnel ထဲကနေ သွားခွင့်ပေးမယ့် traffic တွေကို encrypt လုပ်ဖို့ ACL ရေးပေးရမှာ ဖြစ်ပါတယ်။ tunnel ထဲကနေ end to end သွားခွင့်ပေးမယ့် traffic တွေဖြစ်ပါတယ်။ အခုလုပ်နေတဲ့ lab မှာဆိုရင် YGN Local network ဖြစ်တဲ့ 10.1.1.0/24 နဲ့ SG Local network ဖြစ်တဲ့ 10.2.2.0/24 ဖြစ်ပါတယ်။

### Phase 1 Proposal

```
crypto ikev2 enable outside
crypto ikev2 policy 1
    encryption 3des des
    integrity sha md5
    group 5
    prf sha
    lifetime seconds 86400
```

## IKEv2

Phase 1 proposal သတ်မှတ်တဲ့အခါ method တစ်ခုချင်းစီအတွက် multiple message ပါဝင်နိုင်ပါတယ်။ ဥပမာ encryption method ဆိုပါစို့။ 3des des aes စသာဖြင့် အများကြီးပါဝင်နိုင်ပါတယ်။

```
YGN(config-ikev2-policy)# encryption 3des aes aes-256 aes-192
```

Integrity method မှာလည်း sha, md5 တစ်ပြိုင်နက်တည်း ပါဝင်နိုင်ပါတယ်။ အဲဒီတော့ single proposal မှာ multiple message ကိုသုံးခွင့်ရသွားပါတယ်။ ဒါကြောင့် IKEv1 တုန်းကဆိုရင် proposal တွေအများကြီးရေးရပါတယ်။ အခါ IKEv2 မှာတော့ proposal တစ်ခုဆိုရင် အဆင်ပြေပါပြီ။

## Phase 2 Proposal

```
crypto ipsec ikev2 ipsec-proposal YGN_TO_SG
    protocol esp encryption aes-256
    protocol esp integrity sha-512
```

ဒါကတော့ Phase 2 proposal ဖြစ်ပါတယ်။

## Tunnel Group

```
tunnel-group 198.0.0.2 type ipsec-121
tunnel-group 198.0.0.2 ipsec-attributes
    ikev2 remote-authentication pre-shared-key *****
    ikev2 local-authentication pre-shared-key *****
```

ဒါကတော့ tunnel group create လုပ်တဲ့အဆင့်ဖြစ်ပါတယ်။ IKEv1 တုန်းကလိုပဲ pre-shared key သတ်မှတ်ပေးရပါတယ်။ ဒါပေမယ့် IKEv2 မှာ local authentication နဲ့ remote authentication အတွက် different authentication method ကို သုံးခွင့်ရှိပါတယ်။ ဥပမာ YGN-FW က SG-FW ကို authentication လုပ်တဲ့အခါ AMS@YGN ဆိုတဲ့ key ကိုသုံးပြီး authenticate လုပ်ချင်တယ်။ SG-FW က YGN-FW ကို authenticate လုပ်တဲ့အခါ AMS@SG ဆိုတဲ့ pre-shared key ကိုသုံးချင်တယ်ဆိုပါစို့။ ဒါဆိုရင် အောက်ပါအတိုင်း configure လုပ်နိုင်ပါတယ်။

## IKEv2

```

YGN(config)# tunnel-group 198.0.0.2 type ipsec-l2l
YGN(config)# tunnel-group 198.0.0.2 ipsec-attributes
YGN(config-tunnel-ipsec)# ikev2 remote-authentication pre-
shared-key AMS@SG
YGN(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-
key AMS@YGN

SG(config)# tunnel-group 197.0.0.2 type ipsec-l2l
SG(config)# tunnel-group 197.0.0.2 ipsec-attributes
SG(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-
key AMS@YGN
SG(config-tunnel-ipsec)# ikev2 local-authentication pre-
shared-key AMS@SG

```

## Crypto Map

```

crypto map YGN_MAP 1 match address YGN_TO_SG
crypto map YGN_MAP 1 set peer 198.0.0.2
crypto map YGN_MAP 1 set ikev2 ipsec-proposal YGN_TO_SG
crypto map YGN_MAP interface outside

```

ဒီအဆင့်ကတော့ နောက်ဆုံးအဆင့်ဖြစ်ပါတယ်။ ရှုံးမှာ ရေးခဲ့တဲ့ encryption domain တွေ၊  
remote peer တွေ၊ phase 2 policy တွေကို crypto map တစ်ခုထဲမှာ ပြန်ပေါင်းပေးလိုက်တဲ့  
သဘောဖြစ်ပါတယ်။ ပြီးရင် အဲဒီ crypto map ကို outside interface မှာ assign  
လုပ်ပေးရမှာဖြစ်ပါတယ်။

## Configuring PAT on ASA

```

YGN(config)# object-group network INTERNAL
YGN(config-network-object-group)#   network-object 10.1.1.0
255.255.255.0
YGN(config-network-object-group)# exit

YGN(config)# nat (inside,outside) after-auto source dynamic
INTERNAL interface

```

```

VPCS> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=255 time=2.580 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=255 time=1.916 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=255 time=2.264 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=255 time=3.388 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=255 time=1.749 ms
VPCS>

```

## Configuring NAT exemption

```

YGN(config)# object-group network YGN_LAN
YGN(config-network-object-group)# network-object 10.1.1.0
255.255.255.0
YGN(config-network-object-group)# exit

YGN(config)# object-group network SG_LAN
YGN(config-network-object-group)# network-object 10.2.2.0
255.255.255.0
YGN(config-network-object-group)# exit

YGN(config)# nat (inside,outside) source static YGN_LAN
YGN_LAN destination static SG_LAN SG_LAN no-proxy-arp
route-lookup

```

LAN to LAN traffic တွေကို internet ပေါ်မှာ translate မလုပ်ဖို့အတွက် NAT exemption ရေးပေးပါတယ်။

```

VPCS> ping 10.2.2.10

84 bytes from 10.2.2.10 icmp_seq=1 ttl=64 time=9.113 ms
84 bytes from 10.2.2.10 icmp_seq=2 ttl=64 time=3.646 ms
84 bytes from 10.2.2.10 icmp_seq=3 ttl=64 time=4.350 ms
^C
VPCS>

```

```

YGN# sh crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                               Local                               Remote
Status        Role
2169385          197.0.0.2/500           198.0.0.2/500
READY      INITIATOR
          Encr: 3DES, Hash: SHA96, DH Grp:5, Auth sign: PSK,
          Auth verify: PSK
          Life/Active Time: 86400/1094 sec
Child sa: local selector 10.1.1.0/0 - 10.1.1.255/65535
          remote selector 10.2.2.0/0 - 10.2.2.255/65535
          ESP spi in/out: 0xc2f6d55a/0x4058e1bd
YGN#

```

## IKEv2

```
YGN# show crypto ipsec sa
interface: outside
    Crypto map tag: YGN_MAP, seq num: 1, local addr:
197.0.0.2

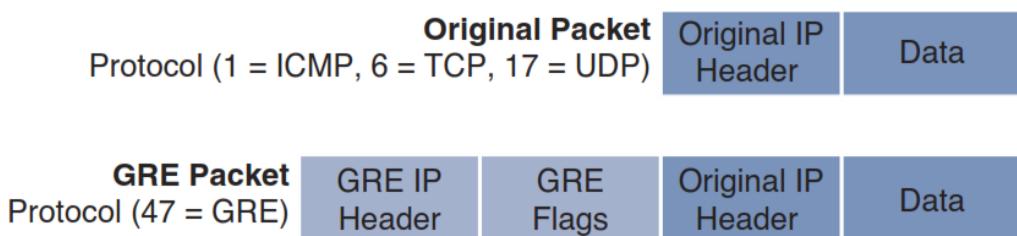
        access-list YGN_TO_SG extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
        local          ident      (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
        remote         ident      (addr/mask/prot/port):
(10.2.2.0/255.255.255.0/0/0)
        current_peer: 198.0.0.2

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```

## Generic Routing Encapsulation (GRE) and IPsec

### What is GRE?

Generic Routing Encapsulation (GRE) ဆိုတာကလည်း tunneling protocol တစ်ခုဖြစ်ပါတယ်။ point to point link တွေအတွက် Network Layer protocol ပေါင်းမြောက်များစွာကို encapsulation လုပ်ပေးနိုင်ပါတယ်။ IP tunnel ထဲမှာ OSPF, EIGRP, IPv6 စတဲ့ protocol ပေါင်း မြောက်များစွာကို encapsulate လုပ်ပေးနိုင်ပါတယ်။ internet ပေါကနေဖြတ်ပြီး Network တစ်ခုနဲ့တစ်ခု packet တွေပို့ကြတဲ့အခါ GRE tunnel ကိုသုံးလေ့ရှုကြပါတယ်။ End point နှစ်ခုကြားမှာ virtual tunnel တစ်ခု တည်ဆောက်လိုက်ပါတယ်။ packet တွေဟာ တည်ဆောက်လိုက်တဲ့ GRE tunnel ထဲကနေ ဖြတ်သန်းသွားလာကြပါတယ်။ GRE header ထဲမှာ အဲဒီ packet တွေကို encapsulate လုပ်လိုက်ပါတယ်။ ပစ္စည်းတစ်ခုကို မပေးပို့ခဲ့ အထူပ် ထုပ်ပြီး ဖုံးပေးလိုက်သလိုမျိုး ဖြစ်ပါတယ်။ GRE ဟာ encapsulation ပဲ support လုပ်ပြီး၊ encryption method တော့ မပါဝင်ပါဘူး။ IPsec သက်သက်ကြီးပဲ အသုံးပြုတဲ့အခါ dynamic routing protocol တွေ အသုံးပြုလို့ မရပြန်ပါဘူး။ ဒါကြောင့် GRE နဲ့ IPsec တွဲပြီးသုံးမှ secure လည်းဖြစ်၊ dynamic routing protocol တွေလည်း အသုံးပြုလို့ ရတဲ့အတွက် အဆင်ပြုပါတယ်။ GRE ကိုသုံးပြီး encapsulate လုပ်ပြီး၊ မလုပ်ခဲ့ packet header ကို လေ့လာကြည့်ပါ။



**IP Packet Before and After GRE**

## GRE over IPsec

GRE over IPSec မှာ IPSec က transport ဖြစ်ပါတယ်။ ဒါကြောင့် LAN to LAN traffic တွေကို GRE က အရင် အထုပ်ထုပ်ပါတယ်။ ဒါကိုတော့ encapsulation လို့ မှတ်နိုင်ပါတယ်။ GRE ကထုပ်ပိုးပေးထားတဲ့ အထုပ်ကို IPsec က encryption လုပ်ပြီး သယ်သွားပါတယ်။

GRE က အရင် အထုပ်ထုပ်ပေးတာကိုတော့ GRE first လို့မှတ်ပါ။ GRE က ထုပ်ပိုးပေးထားတဲ့ အထုပ်ကို IPsec က encryption လုပ်ပြီး သယ်သွားကိုတော့ IPSec is second လို့ မှတ်ပါ။ Proxy-ACL ရေးတဲ့အခါမှာတော့ permit gre host A host B ဆိုပြီး WAN IP နှစ်ခုကိုပဲ ရေးပေးရမှာ ဖြစ်ပါတယ်။ ဥပမာ - permit gre host 100.0.12.2 host 100.0.13.2 လို့ ရေးပေးရမှာ ဖြစ်ပါတယ်။ crypto map ကို physical interface အောက်မှာ apply လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ ဒါကိုတော့ GRE over IPsec with crypto map လို့ ခေါ်ပါတယ်။ နောက်တစ်ခုကတော့ GRE over IPsec with crypto profile ဖြစ်ပါတယ်။ GRE over IPsec with crypto profile မှာ ACL ရေးစရာမလိုပါဘူး။ crypto ipsec profile ဆိုပြီး profile အောက်ပြီး၊ အဲဒီ profile ကို tunnel interface အောက်မှာ tunnel protection ipsec profile ဆိုပြီး apply လုပ်မှာ ဖြစ်ပါတယ်။ ဒီစာအုပ်မှာ ပါဝင်တဲ့ Lab တွေဟာ GRE over IPsec with crypto map and with crypto profile တွေ ဖြစ်ပါတယ်။ IPsec over GRE တစ်ခုမှ မပါဝင်ပါဘူး။

## IPsec over GRE

IPsec over GRE မှာ GRE က transport ဖြစ်ပါတယ်။ ဒါကြောင့် LAN to LAN traffic တွေကို IPsec က အရင် encryption လုပ်ပါတယ်။ IPsec က encryption လုပ်ပေးထားတဲ့ အထုပ်ကို GRE က သယ်သွားပါတယ်။ Proxy-ACL ရေးတဲ့အခါ end to end IP တွေကို ထည့်ရေးရပါတယ်။ ဥပမာ - permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 လို့ ရေးပေးရမှာ ဖြစ်ပါတယ်။ crypto map ကို tunnel interface အောက်မှာ apply လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ **design point of view ကြေည့်ရင် မကောင်းတဲ့အတွက် IPsec over GRE ကို အသုံးမပြုပါဘူး။**

## GRE

IPsec က အရင် encryption လုပ်တာကိုတော့ encryption first လို့မတ်ပါ။ IPsec က encryption လုပ်ပေးထားတဲ့ အထူပ်ကို GRE က သယ်ဆွားကိုတော့ GRE is second လို့မတ်ပါ။

GRE အကြောင်းကို [RFC 1701](#) RFC1702 RFC2784 တို့မှာလည်း လေ့လာနိုင်ပါတယ်။

## GRE Summary

### **GRE = Generic Routing Encapsulation**

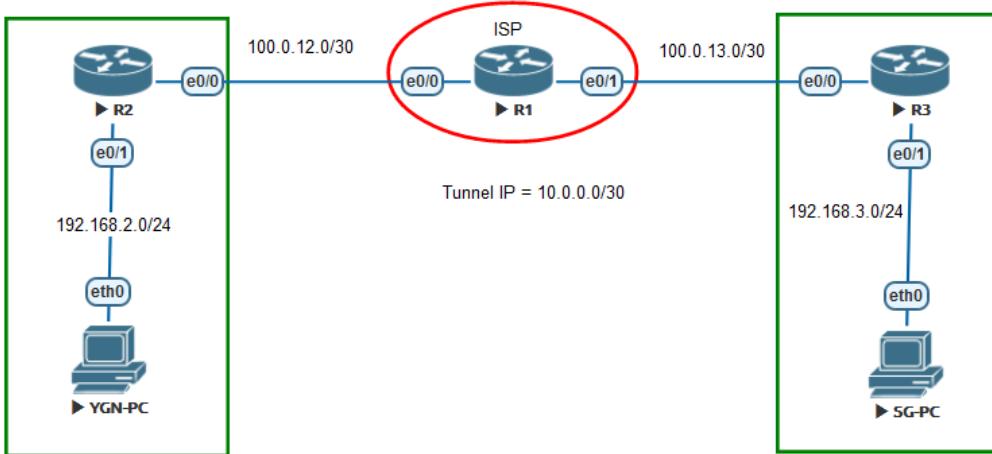
- One of many tunneling protocol
- IP protocol 47: defines GRE packet
- Allows routing information to be passed between connected networks
- GRE does not include any strong security mechanisms to protect its payload. No encryption
- The GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.

### **GRE Tunnel configuration**

- GRE implementation plan:
- Create a tunnel interface
- Specify GRE tunnel mode as the tunnel interface mode (optional)
- Specify the tunnel source and tunnel destination IP address
- Configure an IP address for the tunnel interface

## Lab – 1 GRE over IPsec with Crypto Profiles (IKEv1)

### Diagram



### Task

- Configure GRE tunnel between R2 and R3.
- Use GRE over IPsec with crypto profiles.
- Configure the above GRE tunnel inside an IPsec tunnel between R2 and R3 as follows:
  - Use an ISAKMP Policy with the following options:
  - Pre-Shared Key: AMS\_CISCO
  - Encryption: AES
  - Hash: MD5
  - Diffie-Hellman Group: 2
  - Use a Crypto Map named AMS\_MAP with the following options:
  - GRE Traffic from R2 to R3 and vice-versa should be sent inside the IPsec tunnel.
  - Encrypt the traffic using 128-bit AES.
  - Authenticate the traffic using SHA-1.

- Use ESP Transport mode to save additional encapsulation overhead.
- To prevent the tunnel endpoints from having to do IPsec fragmentation, configure the GRE tunnel IP MTU to 1400 bytes, and set them to adjust the TCP MSS accordingly.

## Solution

### Basic Configuration

#### ISP

```
ISP(config)#interface Ethernet0/0
ISP(config-if)# ip address 100.0.12.1 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#interface Ethernet0/1
ISP(config-if)# ip address 100.0.13.1 255.255.255.252
ISP(config-if)#no shut
R2(config)#interface Ethernet0/0
R2(config-if)# ip address 100.0.12.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface Ethernet0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1

R3(config)#interface Ethernet0/0
R3(config-if)# ip address 100.0.13.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#interface Ethernet0/1
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1
```

## GRE

### GRE configuration

**R2**

```
R2(config)#interface Tunnel0
R2(config-if)# ip address 10.0.0.1 255.255.255.252
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source Ethernet0/0
R2(config-if)# tunnel destination 100.0.13.2
R2(config-if)#exit
```

**R3**

```
R3(config)#interface Tunnel0
R3(config-if)# ip address 10.0.0.2 255.255.255.252
R3(config-if)# ip mtu 1400
R3(config-if)# ip tcp adjust-mss 1360
R3(config-if)# tunnel source Ethernet0/0
R3(config-if)# tunnel destination 100.0.12.2
R3(config-if)#exit
```

### IPsec Configuration

**R2**

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#exit
R2(config)#crypto isakmp key AMS_CISCO address 100.0.13.2

R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(crypto-trans)#mode transport
R2(crypto-trans)#exit

R2(config)#crypto ipsec profile AMS_PRO
R2(ipsec-profile)# set transform-set AMS_SET
R2(ipsec-profile)#exit

R2(config)#interface Tunnel0
R2(config-if)# tunnel protection ipsec profile AMS_PRO
R2(config-if)#exit
```

## R3

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encr aes
R3(config-isakmp)#hash md5
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#crypto isakmp key AMS_CISCO address 100.0.12.2

R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R3(cfg-crypto-trans)#mode transport
R3(cfg-crypto-trans)#exit

R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#mode transport
R2(cfg-crypto-trans)#exit

R2(config)#crypto ipsec profile AMS_PRO
R2(ipsec-profile)# set transform-set AMS_SET
R2(ipsec-profile)#exit

R2(config)#interface Tunnel0
R2(config-if)# tunnel protection ipsec profile AMS_PRO
R2(config-if)#exit
```

## Routing

```
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.0.0.1 0.0.0.0 area 0
R2(config-router)#network 192.168.2.1 0.0.0.0 area 0

R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 10.0.0.2 0.0.0.0 area 0
R3(config-router)#network 192.168.3.1 0.0.0.0 area 0
```

## Verification

```
R2#ping 192.168.3.1 so 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms
R2#
```

```
R2#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 100.0.13.2 port 500
Session ID: 0
IKEv1 SA: local 100.0.12.2/500 remote 100.0.13.2/500
Active
Session ID: 0
IKEv1 SA: local 100.0.12.2/500 remote 100.0.13.2/500
Active
IPSEC FLOW: permit 47 host 100.0.12.2 host 100.0.13.2
Active SAs: 4, origin: crypto map
R2#
```

```
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id status
100.0.12.2   100.0.13.2   QM_IDLE   1002 ACTIVE
100.0.13.2   100.0.12.2   QM_IDLE   1003 ACTIVE

IPv6 Crypto ISAKMP SA
R2#
```

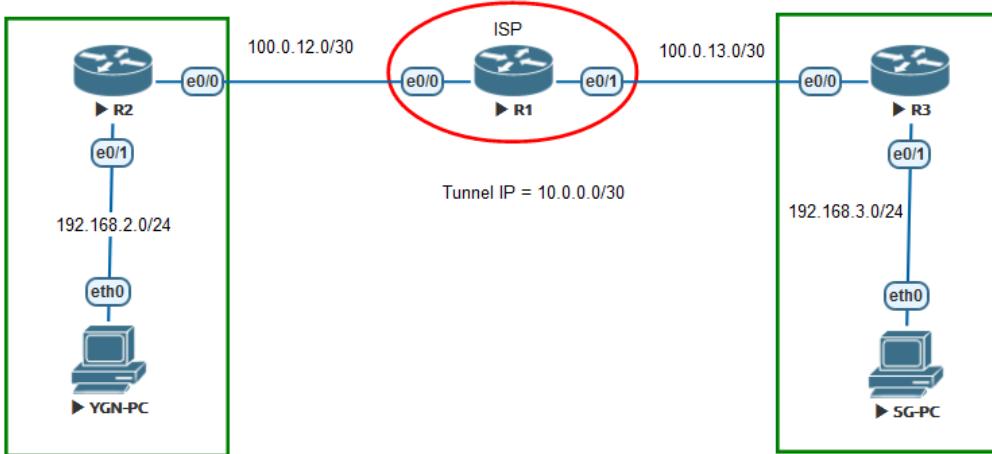
```
R2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 100.0.12.2

protected vrf: (none)
local           ident      (addr/mask/prot/port):
(100.0.12.2/255.255.255.255/47/0)
remote          ident      (addr/mask/prot/port):
(100.0.13.2/255.255.255.255/47/0)
current_peer 100.0.13.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
#pkts decaps: 27, #pkts decrypt: 27, #pkts verify: 27
```

## Lab – 2 GRE over IPsec with Crypto Maps (IKEv1)

### Diagram



### Task

- Configure GRE tunnel between R2 and R3.
- Use GRE over IPsec with Crypto Maps
- Configure the above GRE tunnel inside an IPsec tunnel between R2 and R3 as follows:
  - Use an ISAKMP Policy with the following options:
  - Pre-Shared Key: AMS\_CISCO
  - Encryption: AES
  - Hash: MD5
  - Diffie-Hellman Group: 2
  - Use a Crypto Map named AMS\_MAP with the following options:
  - GRE Traffic from R2 to R3 and vice-versa should be sent inside the IPsec tunnel.
  - Encrypt the traffic using 128-bit AES.
  - Authenticate the traffic using SHA-1.

## GRE

- Use ESP Transport mode to save additional encapsulation overhead.
- To prevent the tunnel endpoints from having to do IPsec fragmentation, configure the GRE tunnel IP MTU to 1400 bytes, and set them to adjust the TCP MSS accordingly.

## Solution

### Basic Configuration

#### ISP

```

ISP(config)#interface Ethernet0/0
ISP(config-if)# ip address 100.0.12.1 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#interface Ethernet0/1
ISP(config-if)# ip address 100.0.13.1 255.255.255.252
ISP(config-if)#no shut
R2(config)#interface Ethernet0/0
R2(config-if)# ip address 100.0.12.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface Ethernet0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1

R3(config)#interface Ethernet0/0
R3(config-if)# ip address 100.0.13.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#interface Ethernet0/1
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1

```

### GRE configuration

#### R2

```

R2(config)#interface Tunnel0
R2(config-if)# ip address 10.0.0.1 255.255.255.252
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source Ethernet0/0

```

## GRE

```
R2(config-if) # tunnel destination 100.0.13.2
R2(config-if) #exit
```

### R3

```
R3(config)#interface Tunnel0
R3(config-if) # ip address 10.0.0.2 255.255.255.252
R3(config-if) # ip mtu 1400
R3(config-if) # ip tcp adjust-mss 1360
R3(config-if) # tunnel source Ethernet0/0
R3(config-if) # tunnel destination 100.0.12.2
R3(config-if) #exit
```

## IPsec Configuration

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp) #exit
R2(config)#crypto isakmp key AMS_CISCO address 100.0.13.2

R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans) #mode transport
R2(cfg-crypto-trans) #exit

R2(config)#ip access-list extended GRE_ACL
R2(config-ext-nacl)#permit gre host 100.0.12.2 host
100.0.13.2
R2(config-ext-nacl) #exit

R2(config)#crypto map AMS_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R2(config-crypto-map) #set peer 100.0.13.2
R2(config-crypto-map) #set transform-set AMS_SET
R2(config-crypto-map) #match address GRE_ACL
R2(config-crypto-map) #exit

R2(config)#interface e0/0
R2(config-if) #crypto map AMS_MAP
R2(config-if) #exit
```

## GRE

### R3

```

R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encr aes
R3(config-isakmp)#hash md5
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#crypto isakmp key AMS_CISCO address 100.0.12.2

R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R3(cfg-crypto-trans)#mode transport
R3(cfg-crypto-trans)#exit
R3(config)#ip access-list extended GRE_ACL
R3(config-ext-nacl)#permit gre host 100.0.13.2 host
100.0.12.2
R3(config-ext-nacl)#exit

R3(config)#crypto map AMS_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R3(config-crypto-map)#set peer 100.0.12.2
R3(config-crypto-map)#set transform-set AMS_SET
R3(config-crypto-map)#match address GRE_ACL
R3(config-crypto-map)#exit
R3(config)#interface e0/0
R3(config-if)#crypto map AMS_MAP
R3(config-if)#exit

```

## Routing

```

R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.0.0.1 0.0.0.0 area 0
R2(config-router)#network 192.168.2.1 0.0.0.0 area 0

R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 10.0.0.2 0.0.0.0 area 0
R3(config-router)#network 192.168.3.1 0.0.0.0 area 0

```

## Verification

```
R2#ping 192.168.3.1 so 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms
R2#
```

```
R2#show crypto session
Crypto session current status

Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 100.0.13.2 port 500
Session ID: 0
IKEv1 SA: local 100.0.12.2/500 remote 100.0.13.2/500 Active
IPSEC FLOW: permit 47 host 100.0.12.2 host 100.0.13.2
Active SAs: 2, origin: crypto map

R2#
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id status
100.0.13.2    100.0.12.2    QM_IDLE      1001 ACTIVE

IPv6 Crypto ISAKMP SA

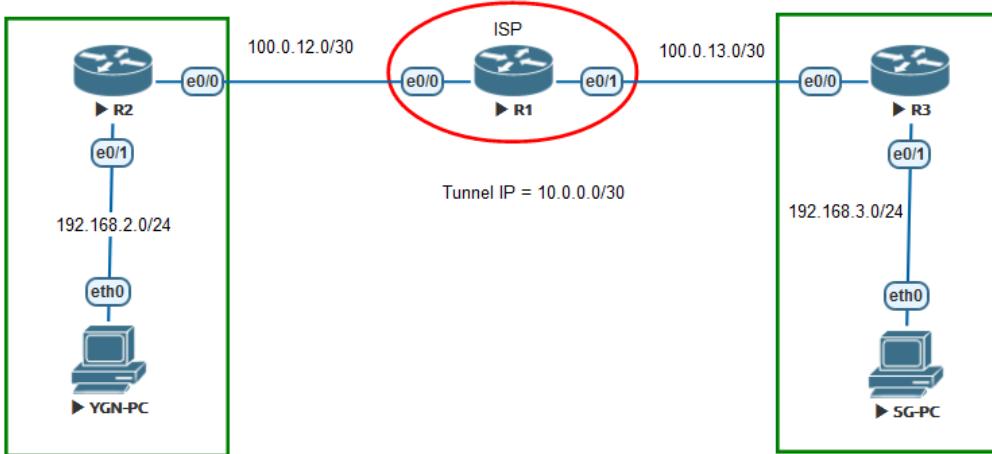
R2#
R2#show crypto ipsec sa

interface: Ethernet0/0
Crypto map tag: AMS_MAP, local addr 100.0.12.2

protected vrf: (none)
local ident (addr/mask/prot/port): (100.0.12.2/255.255.255.255/47/0)
remote          ident          (addr/mask/prot/port):
(100.0.13.2/255.255.255.255/47/0)
current_peer 100.0.13.2 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 41, #pkts encrypt: 41, #pkts digest: 41
#pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
```

## Lab – 3 GRE over IPsec with Crypto Profiles (IKEv2)

### Diagram



### Task

- Configure GRE tunnel between R2 and R3.
- Use IKEv2 with crypto profile for tunnel protection.

### Solution

#### Basic Configuration

##### ISP

```

ISP(config)#interface Ethernet0/0
ISP(config-if)# ip address 100.0.12.1 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#interface Ethernet0/1
ISP(config-if)# ip address 100.0.13.1 255.255.255.252
ISP(config-if)#no shut

R2(config)#interface Ethernet0/0
R2(config-if)# ip address 100.0.12.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface Ethernet0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1

```

## GRE

```
R3(config)#interface Ethernet0/0
R3(config-if)# ip address 100.0.13.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#interface Ethernet0/1
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1
```

## GRE configuration

### R2

```
R2(config)#interface Tunnel0
R2(config-if)# ip address 10.0.0.1 255.255.255.252
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source Ethernet0/0
R2(config-if)# tunnel destination 100.0.13.2
R2(config-if)#exit
```

### R3

```
R3(config)#interface Tunnel0
R3(config-if)# ip address 10.0.0.2 255.255.255.252
R3(config-if)# ip mtu 1400
R3(config-if)# ip tcp adjust-mss 1360
R3(config-if)# tunnel source Ethernet0/0
R3(config-if)# tunnel destination 100.0.12.2
R3(config-if)#exit
```

## IKEv2 Configuration

default IKEv2 proposal နဲ့ default IKEv2 policy ကို အသုံးပြုချင်ရင် keyring ကင် စပ်  
configure လုပ်နိုင်ပါတယ်။

```
R2(config)#crypto ikev2 keyring AMS-GRE-KEY
R2(config-ikev2-keyring)#peer GRE-ROUTER
R2(config-ikev2-keyring-peer)#address 100.0.13.2
R2(config-ikev2-keyring-peer)#pre-shared-key amscisco
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

```
R2(config)#crypto ikev2 profile AMS_PROFILE
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any
statement.
R2(config-ikev2-profile)#match identity remote address
100.0.13.2
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#keyring local AMS-GRE-KEY
R2(config-ikev2-profile)#exit
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#mode transport
R2(cfg-crypto-trans)#exit

R2(config)#crypto ipsec profile IPSEC_PROFILE
R2(ipsec-profile)#set transform-set AMS_SET
R2(ipsec-profile)#set ikev2-profile AMS_PROFILE
R2(ipsec-profile)#exit

R2(config)#interface tunnel 0
R2(config-if)#tunnel protection ipsec profile IPSEC_PROFILE
R2(config-if)#exit
```

```
R3(config)#crypto ikev2 keyring AMS-GRE-KEY
R3(config-ikev2-keyring)#peer GRE-ROUTER
R3(config-ikev2-keyring-peer)#address 100.0.12.2
R3(config-ikev2-keyring-peer)#pre-shared-key amscisco
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit
R3(config)#crypto ikev2 profile AMS_PROFILE
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any
statement.
R3(config-ikev2-profile)#match identity remote address
100.0.12.2
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#keyring local AMS-GRE-KEY
R3(config-ikev2-profile)#exit
R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R3(cfg-crypto-trans)#mode transport
```

## GRE

```
R3(cfg-crypto-trans)#exit
R3(config)#crypto ipsec profile IPSEC_PROFILE
R3(ipsec-profile)#set transform-set AMS_SET
R3(ipsec-profile)#set ikev2-profile AMS_PROFILE
R3(ipsec-profile)#exit
R3(config)#interface tunnel 0
R3(config-if)#tunnel protection ipsec profile IPSEC_PROFILE
R3(config-if)#

```

## Routing

```
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.0.0.1 0.0.0.0 area 0
R2(config-router)#network 192.168.2.1 0.0.0.0 area 0

R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 10.0.0.2 0.0.0.0 area 0
R3(config-router)#network 192.168.3.1 0.0.0.0 area 0

```

## Verification

```
R2#ping 192.168.3.1 so 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms
R2#

```

```
R2#show crypto ikev2 session
IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf
Status
2 100.0.12.2/500 100.0.13.2/500 none/none
READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5,
      Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/520 sec
      Child sa: local selector 100.0.12.2/0 - 100.0.12.2/65535
                  remote selector 100.0.13.2/0 - 100.0.13.2/65535
                  ESP spi in/out: 0x42E98870/0xC9DABB23

IPv6 Crypto IKEv2 Session
R2#

```

```
R2#show crypto session
Crypto session current status

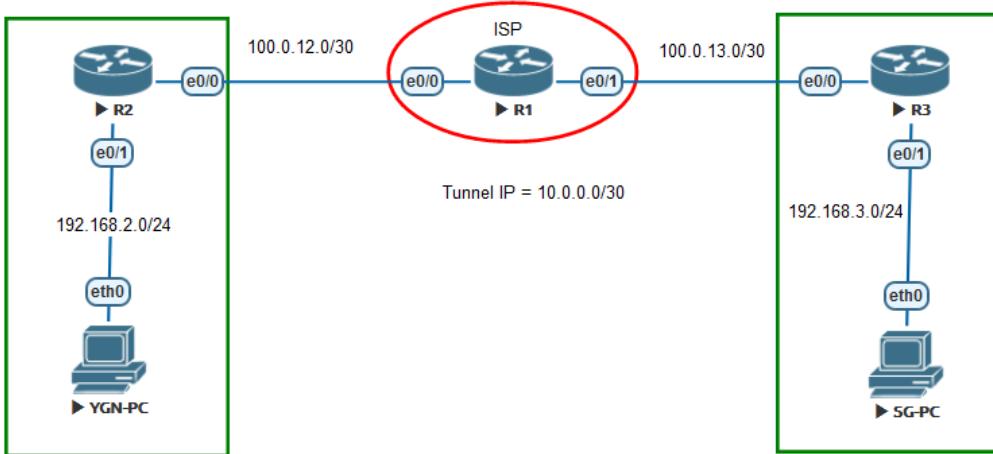
Interface: Tunnel0
Profile: AMS_PROFILE
Session status: UP-ACTIVE
Peer: 100.0.13.2 port 500
Session ID: 2
IKEv2 SA: local 100.0.12.2/500 remote 100.0.13.2/500 Active
IPSEC FLOW: permit 47 host 100.0.12.2 host 100.0.13.2
          Active SAs: 2, origin: crypto map
R2#
R2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 100.0.12.2

protected vrf: (none)
local ident (addr/mask/prot/port): (100.0.12.2/255.255.255.255/47/0)
remote           ident                   (addr/mask/prot/port):
(100.0.13.2/255.255.255.255/47/0)
current_peer 100.0.13.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 38, #pkts encrypt: 38, #pkts digest: 38
#pkts decaps: 33, #pkts decrypt: 33, #pkts verify: 33
```

## Lab – 4 GRE over IPsec with Crypto Maps (IKEv2)

### Diagram



### Task

- Configure GRE tunnel between R2 and R3.
- Use IKEv2 crypto map for protection.

### Solution

#### Basic Configuration

```

ISP
ISP(config)#interface Ethernet0/0
ISP(config-if)# ip address 100.0.12.1 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#interface Ethernet0/1
ISP(config-if)# ip address 100.0.13.1 255.255.255.252
ISP(config-if)#no shut

R2(config)#interface Ethernet0/0
R2(config-if)# ip address 100.0.12.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface Ethernet0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1

```

## GRE

```
R3(config)#interface Ethernet0/0
R3(config-if)# ip address 100.0.13.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#interface Ethernet0/1
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1
```

## GRE configuration

**R2**

```
R2(config)#interface Tunnel0
R2(config-if)# ip address 10.0.0.1 255.255.255.252
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source Ethernet0/0
R2(config-if)# tunnel destination 100.0.13.2
R2(config-if)#exit
```

**R3**

```
R3(config)#interface Tunnel0
R3(config-if)# ip address 10.0.0.2 255.255.255.252
R3(config-if)# ip mtu 1400
R3(config-if)# ip tcp adjust-mss 1360
R3(config-if)# tunnel source Ethernet0/0
R3(config-if)# tunnel destination 100.0.12.2
R3(config-if)#exit
```

## IKEv2 Configuration

```
R2(config)#crypto ikev2 keyring AMS-GRE-KEY
R2(config-ikev2-keyring)#peer GRE-ROUTER
R2(config-ikev2-keyring-peer)#address 100.0.13.2
R2(config-ikev2-keyring-peer)#pre-shared-key amscisco
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

R2(config)#crypto ikev2 profile AMS\_PROFILE

IKEv2 profile MUST have:

1. A local and a remote authentication method.
2. A match identity or a match certificate or match any statement.

## GRE

```
R2(config-ikev2-profile)#match identity remote address
100.0.13.2
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#keyring local AMS-GRE-KEY
R2(config-ikev2-profile)#exit

R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(crypto-crypt-trans)#mode transport
R2(crypto-crypt-trans)#exit

R2(config)#ip access-list extended GRE_ACL
R2(config-ext-nacl)#permit gre host 100.0.12.2 host
100.0.13.2
R2(config-ext-nacl)#exit

R2(config)#crypto map AMS_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
        and a valid access list have been configured.
R2(config-crypto-map)#set peer 100.0.13.2
R2(config-crypto-map)#set transform-set AMS_SET
R2(config-crypto-map)#mat address GRE_ACL
R2(config-crypto-map)#set ikev2-profile AMS_PROFILE
R2(config-crypto-map)#exit

R2(config)#interface Ethernet0/0
R2(config-if)#crypto map AMS_MAP
```

```
R3(config)#crypto ikev2 keyring AMS-GRE-KEY
R3(config-ikev2-keyring)#peer GRE-ROUTER
R3(config-ikev2-keyring-peer)#address 100.0.12.2
R3(config-ikev2-keyring-peer)#pre-shared-key amscisco
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit

R3(config)#crypto ikev2 profile AMS_PROFILE
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate or match any
statement.
R3(config-ikev2-profile)#match identity remote address
100.0.12.2
R3(config-ikev2-profile)#authentication remote pre-share
```

## GRE

```
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#keyring local AMS-GRE-KEY
R3(config-ikev2-profile)#exit

R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R3(cfg-crypto-trans)#mode transport
R3(cfg-crypto-trans)#exit

R3(config)#ip access-list extended GRE_ACL
R3(config-ext-nacl)#permit gre host 100.0.13.2 host
100.0.12.2
R3(config-ext-nacl)#exit

R3(config)#crypto map AMS_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a
peer
      and a valid access list have been configured.
R3(config-crypto-map)#set peer 100.0.13.2
R3(config-crypto-map)#set transform-set AMS_SET
R3(config-crypto-map)#mat address GRE_ACL
R3(config-crypto-map)#set ikev2-profile AMS_PROFILE
R3(config-crypto-map)#exit

R3(config)#interface Ethernet0/0
R3(config-if)#crypto map AMS_MAP
```

## Routing

```
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.0.0.1 0.0.0.0 area 0
R2(config-router)#network 192.168.2.1 0.0.0.0 area 0

R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 10.0.0.2 0.0.0.0 area 0
R3(config-router)#network 192.168.3.1 0.0.0.0 area 0
```

## Verification

```
R2#ping 192.168.3.1 so 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms
R2#
```

```
R2#show crypto session
Crypto session current status

Interface: Ethernet0/0
Profile: AMS_PROFILE
Session status: UP-ACTIVE
Peer: 100.0.0.13.2 port 500
Session ID: 1
IKEv2 SA: local 100.0.0.12.2/500 remote 100.0.0.13.2/500 Active
Session ID: 2
IKEv2 SA: local 100.0.0.12.2/500 remote 100.0.0.13.2/500 Active
IPSEC FLOW: permit 47 host 100.0.0.12.2 host 100.0.0.13.2
    Active SAs: 4, origin: crypto map

R2#
```

```
R2#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id Local                               Remote                               fvrf/ivrf
Status
1          100.0.0.12.2/500                   100.0.0.13.2/500                 none/none
READY
    Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5,
Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/189 sec

Tunnel-id Local                               Remote                               fvrf/ivrf
Status
2          100.0.0.12.2/500                   100.0.0.13.2/500                 none/none
READY
    Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5,
Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/246 sec

IPv6 Crypto IKEv2 SA

R2#
```

## GRE

```
R2#show crypto ipsec sa

interface: Ethernet0/0
  Crypto map tag: AMS_MAP, local addr 100.0.12.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (100.0.12.2/255.255.255.255/47/0)
        remote      ident          (addr/mask/prot/port):
(100.0.13.2/255.255.255.255/47/0)
  current_peer 100.0.13.2 port 500
    PERMIT, flags={origin_is_acl,}
  #pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 45
  #pkts decaps: 44, #pkts decrypt: 44, #pkts verify: 44
```

## IPsec VTI

### SVTI Theory Brief

IPsec Virtual Tunnel Interface (VTI) ဆိုတာကတော့ payload ကို ESP ထဲမှာ တိုက်ရှိက် encapsulate လုပ်ပေးတဲ့ tunnel အမျိုးစားဖြစ်ပါတယ်။ ဒါကြောင့် payload ကို encapsulate လုပ်ဖို့ တခြား transport header မလိုအပ်ပါဘူး။

IPsec VTI ရဲ့ အလုပ်လုပ်ပုံကတော့ GRE tunnel နဲ့ တော်တော်များများ ဆင်တူပါတယ်။ encapsulation overhead က GRE ထက်ပိုနည်းပါတယ်။ သတိထားရမှာတစ်ခုကတော့ payload ကို IPsec ထဲကို တိုက်ရှိက် encapsulate လုပ်တဲ့အတွက် IP သက်သက်ပဲ encapsulation လုပ်ပေးနိုင်ပါတယ်။ တခြား non-IP payload တွေကိုတော့ support မလုပ်ပါဘူး။ ဆိုလိုတဲ့သဘောကတော့ IS-IS routing protocol လိုမျိုး non-IP protocol တွေ IPv4 VTI ပေါ်မှာ run လို့ မရပါဘူး။

VTI Configuration ကလည်း GRE over IPsec tunnel configuration နဲ့ တော်တော်ကြီးကို တူပါတယ်။ IPsec IPv4 or IPsec IPv6 တစ်ခုပဲကွာခြားချက် ရှိပါတယ်။ Phase 1 negotiation ကတော့ တခြား LAN-to-LAN IPsec tunnel တွေအတိုင်းပဲ ဖြစ်ပါတယ်။ ပုံမှန်အားဖြင့်ဆိုရင်တော့ Phase 2 မှာ proxy ACL configure လုပ်ပေးရပါတယ်။ ဒီမှာတော့ IP any any အနေနဲ့ အလိုအလျောက် negotiate လုပ်ပါတယ်။ ဆိုလိုတဲ့သဘောက ACL ရေးစရာမလိုပဲ IP traffic အားလုံးကို protect လုပ်ပေးမှာ ဖြစ်ပါတယ်။ ဒါကြောင့် tunnel ကို maintain လုပ်ဖို့အတွက် လိုအပ်နေတဲ့ IPsec SAs number ကို လျှော့ချြိုးသား ဖြစ်ပါတယ်။ IPsec Transform Set က Tunnel Mode အနေနဲ့ run ကို run ရမှာ ဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ VTI မှာ တခြား transport header မရှိလို့ ဖြစ်ပါတယ်။ GRE မှာဆိုရင် additional IP encapsulation ထပ်ထည့်ပါတယ်။ VTI မှာတော့ GRE လိုမျိုး တခြား additional header ထပ်ထည့်စရာ မလိုပါဘူး။ နောက်တစ်ခုကတော့ VTI က ESP အတွက် ဖြစ်သင့်တဲ့ MTU size ကို အလိုအလျောက် တွက်ချက်ပေးပါတယ်။

## When do you use SVTI?

Site-to-Site VPN မှာ traffic ကို အမြဲတမ်း protection ကို on ထားဖို့ လိုတဲ့အခါတွေမှာ အသုံးပြနိုင်ပါတယ်။ ရှိုးရှိုး IPsec VPN မှာဆိုရင် traffic initiate လုပ်မှ tunnel က up တာဖြစ်ပါတယ်။

နောက်တစ်ခုကတော့ IPsec tunnel ကို သုံးပြီး routing protocol တွေ၊ multicast traffic တွေကို protect လုပ်ပေးလိုတဲ့အခါတွေမှာ SVTI ကို အသုံးပြနိုင်ပါတယ်။ ရှိုးရှိုး IPsec VPN မှာ multicast traffic support မလုပ်ပါဘူး။

နောက်တစ်ခုကတော့ GRE ကို အသုံးမပြုပဲ၊ GRE နေရာ အစားထိုးဖို့ လိုအပ်နေတဲ့အခါတွေမှာ SVTI ကို အသုံးပြနိုင်ပါတယ်။ ဥပမာ- Cisco နဲ့ Cisco မဟုတ်တဲ့ တွေား vendor product တွေနဲ့ Site-to-Site VPN tunnel တည်ဆောက်တဲ့အခါတွေမှာ အသုံးပြနိုင်ပါတယ်။

နောက်တစ်ခုကတော့ tunnel တစ်ခုချင်းစီအလိုက် QoS, security policy တွေ apply လုပ်ချင်တဲ့အခါတွေမှာ Static VTI ကို အသုံးပြနိုင်ပါတယ်။ များသောအားဖြင့်တော့ site အရောတွက် 2 to 50 site အတွက် Cisco နဲ့ Non-Cisco point to point ချိတ်ဆက်တဲ့အခါတွေမှာ အသုံးပြုပါတယ်။

## Advantages and Disadvantages of SVTI

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>➤ Support for IGP dynamic routing protocol over the VPN (EIGRP, OSPF, etc.)</li> <li>➤ Support for multicast</li> <li>➤ Application of features such as NAT, ACLs, and QoS and apply them to clear-text or encrypted text</li> <li>➤ Simpler configuration</li> </ul>	<ul style="list-style-type: none"> <li>➤ No support for non-IP protocols</li> <li>➤ Limited support for multi-vendor</li> <li>➤ IPsec stateful failover not available</li> <li>➤ Similar scaling properties of IPsec and GRE over IPsec</li> <li>➤ Only tunnel mode</li> </ul>

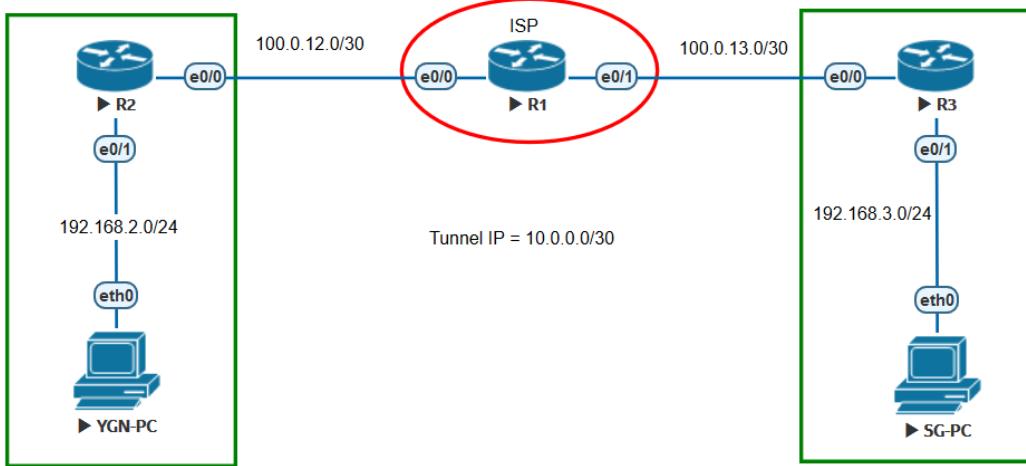
<ul style="list-style-type: none"><li>➤ IPsec sessions not tied to any interface</li><li>➤</li></ul>	
--	--

### Summary of VTI

- Statically configured tunnel via 'tunnel mode ipsec ipv4/ipv6' and tunnel protection
- Always up – IPsec tunnel initiated via configuration and not by traffic
- Interface state tied to underlying crypto socket state (IPsec SA)
- Can initiate and accept only one IPsec SA per VTI, using 'any any' proxy
- local ident (add/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
- remote ident (add/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
- Routing determines traffic to be protected – any packet forwarded to tunnel interface is protected
- IPsec SA re-keyed even in the absence of any traffic

## Lab – 1 IPsec Static Virtual Tunnel Interfaces (IKEv1)

### Diagram



### Task

Configure SVTI for IPsec VPN using following parameter:

- ISAKMP Policy
  - Use AES-256 for encryption
  - Use SHA for integrity
  - Use DH group 2.
  - Use Pre-Shared key AMSCISCO for authentication.
- IPsec
  - Use IPsec Transform set as AMS\_SET with esp-aes and esp-sha-hmac
  - Use IPsec profile as AMS\_PRO
  - Use the IP subnet 10.0.0.0/30 for tunnel interface .1 and .2 respectively.
  - Source the tunnel from e0/0

## Solution

Step 1 – ISAKMP policy

Step 2 – IPsec policy

Step 3 – Create tunnel

Step 4 – routing

### ISP

```
ISP(config)#interface Ethernet0/0
ISP(config-if)# ip address 100.0.12.1 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#interface Ethernet0/1
ISP(config-if)# ip address 100.0.13.1 255.255.255.252
ISP(config-if)#no shut
```

### R2

```
R2(config)#interface Ethernet0/0
R2(config-if)# ip address 100.0.12.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface Ethernet0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1

R2(config)#crypto isakmp policy 1
R2(config-isakmp)# encr aes 256
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)#exit
R2(config)#crypto isakmp key AMS_KEY address 100.0.13.2
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#exit
R2(config)#crypto ipsec profile AMS_PRO
R2(ipsec-profile)# set transform-set AMS_SET
R2(ipsec-profile)#exit
```

```
R2(config)#interface Tunnel0
R2(config-if)# ip address 10.0.0.1 255.255.255.252
R2(config-if)# tunnel source 100.0.12.2
R2(config-if)# tunnel destination 100.0.13.2
R2(config-if)# tunnel mode ipsec ipv4
R2(config-if)# tunnel protection ipsec profile AMS_PRO
```

**R3**

```
R3(config)#interface Ethernet0/0
R3(config-if)# ip address 100.0.13.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#interface Ethernet0/1
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exi
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1

R3(config)#crypto isakmp policy 1
R3(config-isakmp)# encr aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)#exit
R3(config)#crypto isakmp key AMS_KEY address 100.0.12.2
R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R3(cfg-crypto-trans)#exit
R3(config)#crypto ipsec profile AMS_PRO
R3(ipsec-profile)# set transform-set AMS_SET
R3(ipsec-profile)#exit

R3(config)#interface Tunnel0
R3(config-if)# ip address 10.0.0.2 255.255.255.252
R3(config-if)# tunnel source 100.0.13.2
R3(config-if)# tunnel destination 100.0.12.2
R3(config-if)# tunnel mode ipsec ipv4
R3(config-if)# tunnel protection ipsec profile AMS_PRO
```

**Verification**

```
R2#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
R2#
```

```
R2#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
    encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
    hash algorithm: Secure Hash Standard
    authentication method: Pre-Shared Key
    Diffie-Hellman group: #2 (1024 bit)
    lifetime: 86400 seconds, no volume limit

R2#
```

```
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id status
100.0.12.2   100.0.13.2   QM_IDLE    1003 ACTIVE

IPv6 Crypto ISAKMP SA

R2#
```

```
R2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 100.0.12.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 100.0.13.2 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 18, #pkts encrypt: 18, #pkts digest: 18
#pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 100.0.12.2, remote crypto endpt.: 100.0.13.2
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xED5B0BB6(3982166966)
PFS (Y/N): N, DH group: none

inbound esp sas:
    spi: 0xC469F663(3295278691)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: SW:5, sibling_flags 80004040, crypto map: Tunnel0-
head-0
        sa timing: remaining key lifetime (k/sec): (4188173/1401)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
    spi: 0xED5B0BB6(3982166966)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
```

```

conn id: 6, flow_id: SW:6, sibling_flags 80004040, crypto map: Tunnel0-
head-0
    sa timing: remaining key lifetime (k/sec): (4188173/1401)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
R2#

```

```

R2#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
    Hardware is Tunnel
    Internet address is 10.0.0.1/30
    MTU 17878 bytes, BW 100 Kbit/sec, DLY 50000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation TUNNEL, loopback not set
    Keepalive not set
    Tunnel linestate evaluation up
    Tunnel source 100.0.12.2, destination 100.0.13.2
    Tunnel protocol/transport IPSEC/IP
    Tunnel TTL 255
    Tunnel transport MTU 1438 bytes
    Tunnel transmit bandwidth 8000 (kbps)
    Tunnel receive bandwidth 8000 (kbps)
    Tunnel protection via IPsec (profile "AMS_PRO")
    Last input 01:36:17, output never, output hang never
    Last clearing of "show interface" counters 01:50:59
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 3
    Queueing strategy: fifo
    Output queue: 0/0 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
        22 packets input, 2305 bytes, 0 no buffer
        Received 0 broadcasts (0 IP multicasts)
        0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        21 packets output, 2112 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 unknown protocol drops
        0 output buffer failures, 0 output buffers swapped out
R2#

```

## Routing

```

R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.0.0.1 0.0.0.0 area 0
R2(config-router)#network 192.168.2.1 0.0.0.0 area 0
R2(config-router)#exit

R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 10.0.0.2 0.0.0.0 area 0

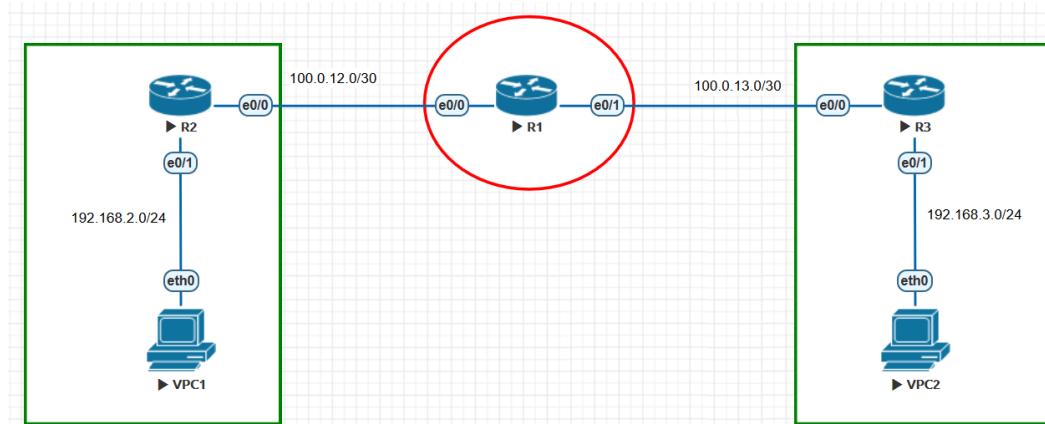
```

```
R3(config-router)#network 192.168.3.1 0.0.0.0 area 0
R3(config-router)#exit
```

```
R2#ping 192.168.3.1 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
R2#
```

## Lab – 2 IPsec Static Virtual Tunnel Interface (IKEv2)

### Diagram



### Task

Configure IPsec SVTI Site-to-Site using following parameter:

- Use AES-CBS-256 for encryption and backup as AES-CBS-256.
- Use SHA-512 for integrity and backup as SHA-256.
- Use DH group 14.
- Use Pre-Shared key AMSCISCO for authentication.
- Use IPsec profile as IPS\_PRO

### Solution

Step 1 – IKEv2 Proposal (optional)

Step 2 – IKEv2 Policy (optional)

Step 3 – Crypto IKEv2 keyring (optional)

Step 4 – Crypto IKEv2 profile

Step 5 – Crypto IPsec Transform Set

Step 6 – Crypto IPsec Profile

## R2 configuration

အဆင့်တစ်အနေနဲ့ IKEv2 proposal configure လုပ်မှာ ဖြစ်ပါတယ်။ ရှိပြီးသား IKEv2 proposal ကို သုံးချင်ရင်လည်းရသလို့၊ သီးသန့် proposal configure လုပ်လည်း ရပါတယ်။ ရှိပြီးသား proposal ကို show crypto ikev2 proposal default နဲ့စစ်ကြည့်နိုင်ပါတယ်။

```
R2#show crypto ikev2 proposal default
IKEv2 proposal: default
    Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
    Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
    PRF         : SHA512 SHA384 SHA256 SHA1 MD5
    DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
R2#
```

### Step - 1 IKEv2 Proposal

```
R2(config)#crypto ikev2 proposal AMS-PROPOSAL
R2(config-ikev2-proposal)#encryption aes-cbc-256
R2(config-ikev2-proposal)#integrity sha256
R2(config-ikev2-proposal)#group 14
R2(config-ikev2-proposal)#exit
```

အဆင့်နှစ်ကတော့ IKEv2 policy configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ ဒီအဆင့်ကလည်း optional ဖြစ်တဲ့အတွက်၊ ရှိပြီးသား default ကို သုံးချင်ရင် သုံးလို့ရပါတယ်။

```
R2#show crypto ikev2 policy default
IKEv2 policy : default
    Match fvrf : any
    Match address local : any
    Proposal    : default
R2#
```

သင့်တော်သလို့ configure လုပ်ချင်တယ်ဆိုရင်တော့ အောက်ပါအတိုင်း လုပ်ပေးရမှာ ဖြစ်ပါတယ်။

### Step - 2

```
R2(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R2(config-ikev2-policy)#proposal AMS_POLICY
```

အဆင့်သုံးကတော့ IKEv2 keyring configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ Key သတ်မှတ်တဲ့ အခါမှာလည်း တစ်ဘက်နဲ့တစ်ဘက် မတူလည်း ရပါတယ်။ ဥပမာ - R2 က R2AMSCISCO လို့ သုံးပြီး၊ R3 က R3AMSCISCO လို့ မတူအောင်ထားလည်း အဆင်ပြေပါတယ်။ အခုလုပ်နေတဲ့ Lab မှာတော့ တူအောင်ထားလိုက်ပါတယ်။

#### Step - 3 Crypto IKEv2 keyring

```
R2(config)#crypto ikev2 keyring AMSKEY
R2(config-ikev2-keyring)#peer R3
R2(config-ikev2-keyring-peer)#address 100.0.13.2
R2(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
```

##### For asymmetric key

```
R2(config-ikev2-keyring-peer)#pre-shared-key local R2AMSCISCO
R2(config-ikev2-keyring-peer)#pre-shared-key remote R3AMSCISCO
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

အဆင့်လေးကတော့ IKEv2 profile configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ IKEv2 profile ထဲမှာ match ဖြစ်တဲ့ IKE ID သတ်မှတ်ခြင်း၊ local နဲ့ remote အတွက် authentication method သတ်မှတ်ခြင်း၊ ရှေ့မှာ configure လုပ်ခဲ့တော့တွေကို reference သတ်မှတ်ခြင်း တို့ ပါဝင်ပါတယ်။

#### Step - 4 Crypto IKEv2 profile

```
R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any statement.
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#match identity remote address 100.0.13.2
R2(config-ikev2-profile)#keyring local AMSKEY
R2(config-ikev2-profile)#exit
```

အဆင့်ငါးကတော့ IPsec transform set configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ ရှိပြီးသားသုံးချင်ရင်လည်း သုံးလို့ရပါတယ်။

```
R2#sh crypto ipsec transform-set default
{ esp-aes esp-sha-hmac }
  will negotiate = { Transport, },
```

သင့်တော်သလို configure လုပ်မယ်ဆိုရင်တော့ အောက်ပါအတိုင်းလုပ်ပေးရမှာ ဖြစ်ပါတယ်။

#### Step 5 – Crypto IPsec Transform Set

```
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#exit
```

အဆင့်ခြောက်ကတော့ IKEv2 profile နဲ့ transform set ကို reference ပြန်လုပ်ဖို့ IPsec profile configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ IPsec profile မှာလည်း default IPsec profile ရှိပါတယ်။

```
R2#sh crypto ipsec profile default
IPSEC profile default
    Security      association      lifetime:        4608000
    kilobytes/3600 seconds
    Responder-Only (Y/N) : N
    PFS (Y/N) : N
    Mixed-mode : Disabled
    Transform sets={
        default: { esp-aes esp-sha-hmac } ,
    }

R2#
Step - 6 Crypto IPsec profile
R2(config)#crypto ipsec profile IPS_PRO
R2(ipsec-profile)#set ikev2-profile AMS_PRO
R2(ipsec-profile)#set transform-set AMS_SET
R2(ipsec-profile)#exit
```

အဆင့်ခုနှစ်ကတော့ tunnel configure လုပ်ပြီး၊ IPsec profile နဲ့ protect လုပ်ပေးရုံးပဲ ဖြစ်ပါတယ်။

#### Step - 7 Create tunnel interface

```
R2(config)#interface Tunnel0
R2(config-if)#ip address 10.0.0.1 255.255.255.252
R2(config-if)#tunnel source Ethernet0/0
R2(config-if)#tunnel destination 100.0.13.2
R3(config-if)#tunnel mode ipsec ipv4
R2(config-if)#tunnel protection ipsec profile IPS_PRO
R2(config-if)#exit
```

အဆင့်ရှစ်ကတော့ LAN to LAN အဆက်သွယ်လုပ်နည်း static route, dynamic route run ပေးရမှာ ဖြစ်ပါတယ်။

#### **Step - 6 routing**

```
R2(config)#router eigrp 10
R2(config-router)#network 10.0.0.1 0.0.0.0
R2(config-router)#network 192.168.2.1 0.0.0.0
R2(config-router)#exit
```

### **R3 configuration**

#### **Step - 1 IKEv2 Proposal**

```
R3(config)#crypto ikev2 proposal AMS-PROPOSAL
R3(config-ikev2-proposal)#encryption aes-cbc-256
R3(config-ikev2-proposal)#integrity sha256
R3(config-ikev2-proposal)#group 14
R3(config-ikev2-proposal)#exit
```

#### **Step - 2**

```
R3(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R3(config-ikev2-policy)#proposal AMS_POLICY
```

#### **Step - 3 Crypto IKEv2 keyring**

```
R3(config)#crypto ikev2 keyring AMSKEY
R3(config-ikev2-keyring)#peer R2
R3(config-ikev2-keyring-peer)#address 100.0.12.2
R3(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit
```

#### **Step - 4 Crypto IKEv2 profile**

```
R3(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any statement.
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#match identity remote address 100.0.12.2
R3(config-ikev2-profile)#keyring local AMSKEY
R3(config-ikev2-profile)#exit
```

#### **Step 5 - Crypto IPsec Transform Set**

```
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#exit
```

**Step - 6 Crypto IPsec profile**

```
R3(config)#crypto ipsec profile IPS_PRO
R3(ipsec-profile)#set ikev2-profile AMS_PRO
R3(ipsec-profile)#set transform-set AMS_SET
R3(ipsec-profile)#exit
```

**Step - 7 Create tunnel interface**

```
R3(config)#interface Tunnel0
R3(config-if)#ip address 10.0.0.2 255.255.255.252
R3(config-if)#tunnel source Ethernet0/0
R3(config-if)#tunnel destination 100.0.12.2
R3(config-if)#tunnel mode ipsec ipv4
R3(config-if)#tunnel protection ipsec profile IPS_PRO
R3(config-if)#exit
```

**routing**

```
R3(config)#router eigrp 10
R3(config-router)# network 10.0.0.2 0.0.0.0
R3(config-router)# network 192.168.3.1 0.0.0.0
R3(config-router)#exit
```

## Verification

```
R2#ping 192.168.3.1 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms
R2#
```

```
R2#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id Local                  Remote                  fvrf/ivrf      Status
1          100.0.12.2/500          100.0.13.2/500        none/none     READY
    Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign:
    PSK, Auth verify: PSK
    Life/Active Time: 86400/309 sec

IPv6 Crypto IKEv2 SA

R2#
```

```
R2#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 100.0.12.2

    protected vrf: (none)
    local ident (addr/mask/prot/port): (100.0.12.2/255.255.255.255/47/0)
    remote ident (addr/mask/prot/port): (100.0.13.2/255.255.255.255/47/0)
    current_peer 100.0.13.2 port 500
        PERMIT, flags={origin_is_acl,}
        #pkts encaps: 109, #pkts encrypt: 109, #pkts digest: 109
        #pkts decaps: 111, #pkts decrypt: 111, #pkts verify: 111
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts compr. failed: 0
        #pkts not decompressed: 0, #pkts decompress failed: 0
        #send errors 0, #recv errors 0
```

### Useful verification commands

```
R2#show run | section crypto
R2#show crypto ikev2 profile
R2#show crypto ikev2 proposal
R2#show crypto engine connections active
```

အခုခိုရင် pre-shared key (PSK) ကိုသုံးပြီး FlexVPN site-to-site with tunnel interface configuration တော့ အောင်မြင်သွားပါပြီ။ GRE ကိုလည်း အသုံးပြုလို့ ရပါတယ်။

## FlexVPN

### What is FlexVPN?

Flex VPN ဆိတာကတော့ IKEv2 ကို အခြေခံပြီး၊ site-to-site, remote-access, hub-spoke and spoke-spoke topologies တွေအားလုံးကို ပေါင်းစပ်ထားတဲ့ unified VPN ဖြစ်ပါတယ်။ FlexVPN အနေနဲ့ multiple framework ကို တစ်ခုတည်းဖြစ်အောင် ပေါင်းစပ်ထားတာ ဖြစ်ပါတယ်။ အဲဒီတော့ CLI point of view ကဗြိုလ်ရင် ပြီးပြည့်စုံတဲ့ VPN အမျိုးစား တစ်ခု ဖြစ်လာပါတယ်။ ကိုယ်သုံးချင်တဲ့ function ပေါ်မှတည်ပြီး extend လုပ်လို့ရတဲ့အတွက် flexible ဖြစ်ပါတယ်။ ဒါကြောင့် FlexVPN ဟာ simple ဖြစ်သလို၊ modular framework လည်း ဖြစ်ပါတယ်။ FlexVPN ဟာ IKEv2 ကို အခြေခံပြီး အလုပ် လုပ်တာ ဖြစ်တဲ့အတွက် FlexVPN မှာ အဓိကကတော့ IKEv2 ပဲ ဖြစ်ပါတယ်။

### VPN Technology Selection

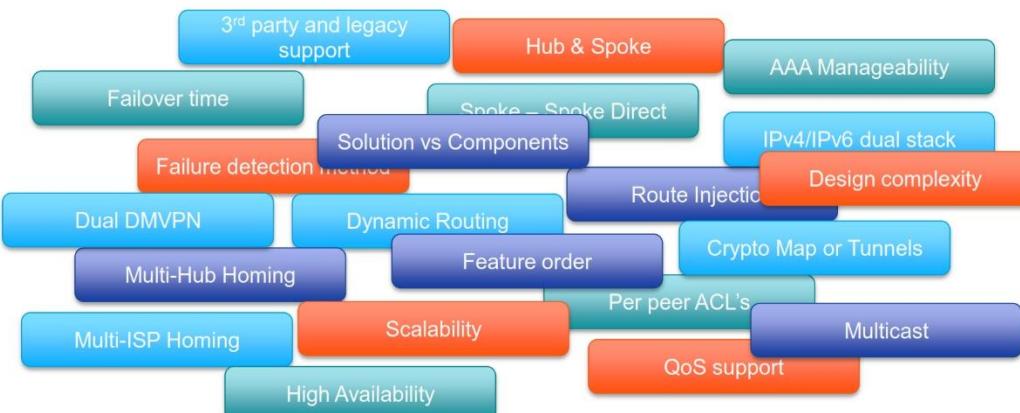
Cisco IPsec VPN solution အမျိုးစားတွေဟာ အများကြီးရှိပါတယ်။ အဲဒီတွေကတော့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

- Static crypto maps
- Dynamic crypto maps
- Legacy EzVPN (Easy VPN) based on crypto maps
- GRE interfaces with crypto maps on WAN interface
- GRE interfaces with tunnel protection
- IPsec VTI (virtual tunnel interface): static and dynamic VTI
- DMVPN (dynamic multipoint VPN)
- Enhanced EzVPN based on IPsec VTI
- GET VPN (group encrypted transport VPN) တို့ဖြစ်ပါတယ်။

Solution တစ်ခုခြင်းများ မတူညီတဲ့ ရည်ရွယ်ချက်တွေ၊ မတူညီတဲ့ feature တွေ၊ မတူညီတဲ့ configuration တည်ဆောက်ပုံတွေ ရှိပါတယ်။ တစ်ခုနဲ့တစ်ခုကလည်း ဆက်နွယ်မှုမရှိပဲ သိုးသန့်ဆဲ ရပ်တည်နေကြတာ ဖြစ်ပါတယ်။ ဥပမာ - DMVPN ဆိုရင် multipoint GRE ကို

## Flex VPN

အသုံးပြုပါတယ်။ overlay network ပေါက်နေဖြတ်ပြီး dynamic routing protocol တွေ အသုံးပြုလို ရပါတယ်။ ဒါပေမယ့် AAA (authentication, authorization, and accounting) support မလုပ်သလို၊ per-user or per-peer policy လည်း အသုံးပြုလို မရပါဘူး။ EzVPN ကကျတော့ point-to-point IPsec VTI ကို အသုံးပြုပါတယ်။ AAA (authentication, authorization, and accounting) support လုပ်သလို၊ per-user or per-peer policy လည်း အသုံးပြုလို ရပါတယ်။ ဒါပေမယ့် EzVPN မှာကျ overlay network ပေါက်ဖြတ်ပြီး dynamic routing protocol တွေ အသုံးပြုဖို့အတွက် dynamic overlay routing ကို support မလုပ်ပါဘူး။ အဲဒီတော့ requirement ကို အခြေခံပြီး device တစ်ခုပေါ်မှာ IPsec VPN solution မျိုးစုံကို configure လုပ်ဖို့ဆိတာ မလွယ်ကူလွယ်ပါဘူး။ ဘယ် IPsec VPN solution ကို အသုံးပြုရင် ကောင်းမလဲ စဉ်းစားတဲ့အခါ စဉ်းစားစရာတွေကလည်း များလှပါတယ်။ Hub & spoke, Spoke to spoke direct traffic သွားခွင့် ရှိ၊ မရှိ၊ third party device တွေနဲ့ ချိတ်ဆက်ခွင့် ရှိ၊ မရှိ၊ multicast support လုပ်၊ မလုပ်၊ dynamic routing သုံးလို့ ရဲ၊ မရ၊ AAA support လုပ်၊ မလုပ် multi-Hub သုံးလို့ ရဲ၊ မရ၊ multiple ISP သုံးလို့ ရဲ၊ မရ၊ scalability ကောင်း၊ မကောင်း စတာတွေကို ထည့်သွင်းပြီး စဉ်းစားရပါတယ်။



ဒီပြဿနာတွေဖြေရှင်းဖို့အတွက် IKEv2 အနေနဲ့ multiple RFC တွေကို ပေါင်းပြီး function တွေအများကြီးကို ပေါင်းစပ်ပေးလိုက်ပါတယ်။ အဲဒီတော့ Cisco အနေနဲ့ IKEv2 ကို အသုံးပြုပြီး different VPN solution တွေကို တစ်စုံတစ်စုံတည်းတည်းဖြစ်အောင် develop လုပ်လိုက်တော့

## Flex VPN

FlexVPN ဆိတ် ဖြစ်ပေါ်လာပါတယ်။ **same configuration, same basic building block** အောက်မှာ solution အားလုံးကို ပေါင်းစပ်ပေးလိုက်တာ ဖြစ်ပါတယ်။

ဒါနောက် FlexVPN ဆိတ် ဘာလဲလို့ မေးလာခဲ့ရင် အခုလို ဖြေဆိုနိုင်ပါတယ်။

**FlexVPN ဆိတ် IKEv2 ကို အခြေခံပြီး၊ multiple VPN topology ကို create လုပ်ပေးတဲ့ unified Cisco IOS VPN solution ဖြစ်ပါတယ်။**

Solution position point of view ကြည့်ရင် FlexVPN တစ်ခုထဲလေ့လာလိုက်တာနဲ့ VPN topology ပါဝင်ပါတယ်။ Cisco အနေနဲ့ VPN solution တွေကို နှင့်ယူဉ်ပြထားတာကို လေ့လာကြည့်ပါ။

	Interop.	Dynamic Routing	IPsec Routing	Spoke to Spoke Direct	Remote Access	Simple Failover	Source Failover	Config Push	Per-Peer Config	Per-Peer QoS	Full AAA Mgmt
Easy VPN	No	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Complex
DMVPN	No	Yes	No	Yes	No	Partial	No	No	No	Group	No
Crypto Map	Yes	No	Yes	No	Yes	Poor	No	No	No	No	No
FlexVPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

### Benefits of FlexVPN

FlexVPN ရဲ့ ကောင်းကျိုးတွေကလည်း အများကြီးရှိပါတယ်။ အောက်မှာ လေ့လာကြည့်ပါ။

- Standards-based, interoperable with non-Cisco IKEv2 implementations
- Support for multiple VPN topologies such as point-to-point, remote-access, hub-spoke, and dynamic mesh
- Multiple VPN technologies under one command line interface (CLI)
- Reduction in training to learn multiple VPN technologies
- Unified configuration and show commands, underlying interface infrastructure, and feature across the supported VPN topologies
- Support for per-user or per-peer policy
- Support for dynamic overlay routing

## Flex VPN

- Integration with Cisco IOS AAA infrastructure
- Support for GRE and native IPsec encapsulations with auto-detection of encapsulation protocol
- Support for IPv4 and IPv6 overlay and underlay with auto-detection of IP transport type

### When do you use FlexVPN?

Customer ၂ IKEv2 feature တွေလိုအပ်နေတဲ့အတွက် IKEv2 ကိုလည်း အသုံးပြုချင်နေတဲ့အခါတွေ unified CLI ကို အသုံးပြုပြီး site-to-site, remote-access, hub-spoke and spoke-spoke topologies တွေကို အသုံးပြုချင်တဲ့အခါတွေ site တွေက 50 to 10,000 အထိ ရှုပြုး၊ hub and spoke, spoke to spoke large scale deployment လိုအပ်နေတဲ့အခါတွေမှာ အသုံးပြုနိုင်ပါတယ်။ နောက်တစ်ခုကတော့ Cisco နဲ့ Cisco မဟုတ်တဲ့ တွေး vendor နဲ့ချိတ်ဆက်တဲ့အခါတွေမှာ အသုံးပြုနိုင်ပါတယ်။

### FlexVPN Building Blocks

FlexVPN configuration လုပ်တဲ့အခါ အမိက အပိုင်းသုံးပိုင်းပါဝင်ပါတယ်။ အဲဒါတွေကတော့-

1. IKEv2
2. Cisco IOS point-to-point (P2P) tunnel interfaces
3. Cisco IOS AAA infrastructure တို့ဖြစ်ပါတယ်။

IKEv2 အကြောင်း လေ့လာခဲ့ပြီမှာ ဒီနေရာမှာ ထပ်မရေးတော့ပါဘူး။

### Cisco IOS Point-to-Point Tunnel Interfaces

FlexVPN အနေနဲ့ VPN topology အားလုံးအတွက် per-peer point-to-point (P2P) tunnel interface ကို အသုံးပြုပါတယ်။ FlexVPN initiator မှာ P2P tunnel interface ကို statically configure လုပ်ပေးရပါတယ်။ FlexVPN responder ၃ virtual-template interface ကတဆင့် dynamically detect လုပ်ပြီး clone interface တွေဖြစ်တဲ့ virtual-access interface တွေကို create လုပ်ပါတယ်။ FlexVPN ၂ အသုံးပြုနေတဲ့ point-to-point tunnel interface table 0 -2 မှာ လေ့လာကြည့်ပါ။

P2P Tunnel Interface Type	Usage
Static GRE interface (tunnel mode gre)	Initiator
Static IPsec VTI (sVTI) (tunnel mode IPsec)	Initiator
Virtual-template interface of type tunnel with GRE encapsulation (tunnel mode IPsec)	
Native IPsec encapsulation (tunnel mode IPsec)	
Auto-detection of tunnel mode and transport protocol (IPv4 /IPv6)	

**Table 0 – 1 P2P Tunnel Interface Used by FlexVPN**

လက်တွေ့ configure လုပ်တဲ့အခါမှာ အသေးစိတ်ထပ်မံလေ့လာရမှာ ဖြစ်ပါတယ်။

### Configuring P2P interface

P2P GRE Tunnel Interface Configuration
R3(config)#interface Tunnel0 R3(config-if)# ip address 192.168.255.3 255.255.255.0 R3(config-if)# tunnel source Ethernet0/0 R3(config-if)# tunnel destination 100.0.0.12.2 R3(config-if)# tunnel protection ipsec profile IPSEC_PRO

ဒါကတော့ P2P GRE interface configuration ဥပမာ ဖြစ်ပါတယ်။ running config ကိစစ်တဲ့အခါ tunnel mode gre ip command တော့ ပြင်ရမှာ မဟုတ်ပါဘူး။

P2P IPsec VTI Tunnel Interface Configuration
R3(config)#interface Tunnel0 R3(config-if)# ip address 192.168.255.3 255.255.255.0 R3(config-if)# tunnel source Ethernet0/0 R3(config-if)# tunnel destination 100.0.0.12.2 R3(config-if)# tunnel mode ipsec ipv4 R3(config-if)# tunnel protection ipsec profile IPSEC_PRO

ဒါကတော့ P2P IPsec VTI configuration ဥပမာ ဖြစ်ပါတယ်။

### Configuring virtual-template interface

Virtual-template Interface Configuration
R2(config)#interface Virtual-Template1 type tunnel R2(config-if)# ip unnumbered Loopback1 R2(config-if)# ip nhrp network-id 1 R2(config-if)# ip nhrp redirect

```
R2(config-if)# tunnel source Ethernet0/0
R2(config-if)# tunnel protection ipsec profile IPSEC_PRO
R2(config-if)#exit
```

### Virtual-template configure လုပ်တဲ့အခါ -

**Tunnel destination command** လုံးဝမထည့်ရပါဘူး။ initiator ကပိုလိုက်တဲ့ incoming IPsec Security Association proposal ကိုအခြေခံပြီး၊ tunnel destination address ကို clone interface ဖြစ်တဲ့ virtual-access interface က ဖန်တီးသွားမှာ ဖြစ်ပါတယ်။

**Tunnel source command** ကတော့ ထည့်ချင်ထည့်၊ မထည့်ချင်နေ ရပါတယ်။ ဘာကြောင့်လဲဆိုတော့ initiator တွေက responder ရဲ့ IP address ကို tunnel destination 100.0.12.2 ဆိုပြီး ရိုက်ထားတဲ့အတွက် Security Association proposal ထဲမှာ အဲဒီ 100.0.12.2 ကို destination အနေနဲ့ responder ဆီကို ပိုမှာ ဖြစ်ပါတယ်။ responder မှာလည်း 100.0.12.2 က အဆင့်သင့်ဖြစ်နေရင် အဆင်ပြေပါပြီ။ သီးသန့် tunnel source ဆိုပြီး ရိုက်စရာမလိုပါဘူး။

**ip unnumbered command** ကတော့ မဖြစ်မနေ ရိုက်ပေးရမှာ ဖြစ်ပါတယ်။ overlay IP address ကို သတ်မှတ်ပေးတာ ဖြစ်ပါတယ်။ clone interface အားလုံးက virtual-interface မှာ ရိုက်ထားတဲ့ command တွေအားလုံးကို ယူသုံးမှာ ဖြစ်ပါတယ်။ သူများ IP ကို တားသုံးနိုင်ဖို့အတွက် ip unnumbered command လိုကို လိုအပ်ပါတယ်။

**tunnel protection command** ကတော့ IPsec enable လုပ်ပေးလိုက်တာဖြစ်ပါတယ်။

အခုရှင်းပြနေတဲ့ ဥပမာမှာ tunnel mode မထည့်ထားတဲ့အတွက် default က GRE ဖြစ်ပါတယ်။ show interfaces virtual-template 1 | include Tunnel protocol ဆိုပြီး စစ်ကြည့်နိုင်ပါတယ်။ tunnel mode ipsec ဆိုပြီး ပြောင်းချင်ပြောင်းလိုရပါတယ်။ tunnel encapsulation mode နဲ့ transport IP protocol ကို auto ထားချင်လည်း ထားလိုရပါတယ်။

```
R2(config)#crypto ikev2 profile AMS_PRO
R2(config-ikev2-profile)#virtual-template 1 mode auto
```

IOS version နှင့်နေရာင်တော့ mode auto command ရှိက်လို့ မရပါဘူး။ IOS version 15.4 ဆိုရင် ရှိက်လို့ ရပါတယ်။

### Cisco IOS AAA Infrastructure

AAA ဆိုတာကတော့ Authentication, Authorization နဲ့ Accounting တို့ဖြစ်ပါတယ်။ FlexVPN က AAA client အနေနဲ့ register လုပ်ပါတယ်။ FlexVPN AAA operation နဲ့ support လုပ်တဲ့ database တွေကို လေ့လာကြည့်ပါ။

FlexVPN AAA Operation	Supported AAA Database
EAP authentication	External AAA server for standard-based EAP External and local AAA for Anyconnect-EAP
AAA-based pre-shared key	External AAA server
User authorization	External AAA server and local AAA database
Group authorization	External AAA server and local AAA database
Implicit authorization	External AAA server
Accounting	External AAA server

**Table 0 – 2 FlexVPN AAA Operations and Supported AAA Databases**

### Benefits of Per-Peer P2P Tunnel Interface

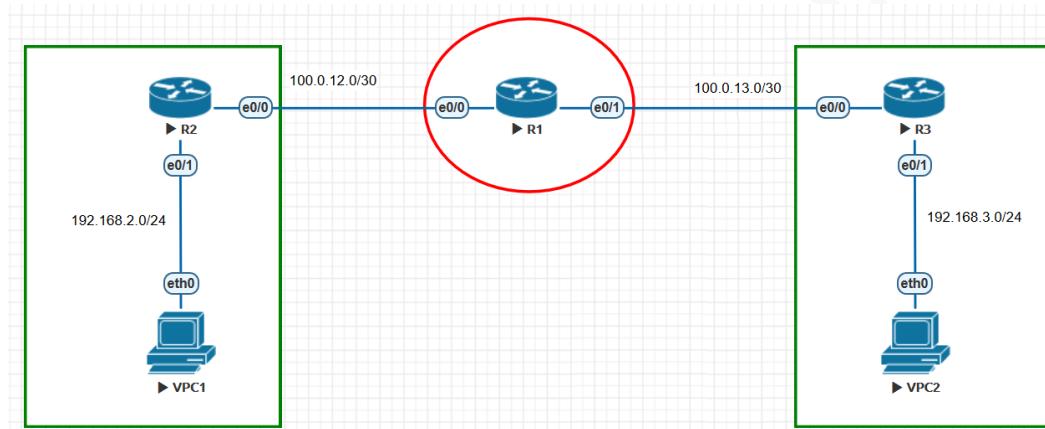
FlexVPN အနေနဲ့ session အားလုံးအတွက် dedicated P2P interface ကို အသုံးပြုပါတယ်။ ဆိုလိုတဲ့သဘောကတော့ peer တစ်ခုခြင်းနဲ့အတွက် dedicated P2P interface ကို အသုံးပြုပါတယ်။ Cisco IOS feature တော်တော်များများကလည်း interface မှာ apply လုပ်တာ ဖြစ်ပါတယ်။ ဥပမာ - quality of service (QoS), access control List (ACL) တို့ ဖြစ်ပါတယ်။ per-peer or per-session interface ကို အသုံးပြုတဲ့အတွက် peer တစ်ခုခြင်းနဲ့အတွက် interface feature တွေအားလုံး apply လုပ်လို့ ရသွားပါတယ်။ ဥပမာ different QoS policy or ACL တွေကို peer တွေပေါ်မှာ apply လုပ်လို့ ရသွားပါတယ်။ ဒါတွေဟာ Per-Peer P2P Tunnel Interface ကို အသုံးပြုရခြင်းရဲ့ ကောင်းကျိုးတွေ ဖြစ်ပါတယ်။

## Flex VPN

အချက်လောလောဆယ်မှတော့ multipoint interface ကို အသုံးပြုနေတဲ့ DMVPN မှာ per-peer or per-session အတွက် စိတ်ကြိုက် policy ကို အသုံးပြုလို့ မရပါဘူး။

### Lab – 1 Flex VPN Site-to-Site with Crypto Map

#### Diagram



#### Lab objective

ဒဲ Lab ရဲရည်ရွယ်ချက်ကတော့ practice များများ လုပ်ဖြစ်ဖို့အတွက်သက်သက်ပဲ ဖြစ်ပါတယ်။

Cisco ကလည်း FlexVPN မှာ crypto map ကိုသုံးတာကို recommend မလုပ်ပါဘူး။

#### Task

Configure Flexvpn Site-to-Site using crypto map with following parameter:

IKEv2 Proposal	
Encryption	aes-cbc-256
Integrity	sha256
Group	group 14

IKEv2 Policy	
Match fvrf	global
Match address local	any
Proposal	AMS-PROPOSAL

<b>IKEv2 Keyring</b>	
<b>Peer</b>	<b>R2 and R3</b>
<b>address</b>	<b>100.0.12.2 and 100.0.13.2</b>
<b>pre-shared-key</b>	<b>AMSCISCO</b>

<b>IKEv2 Profile</b>	
<b>Profile Name</b>	<b>AMS_PRO</b>
<b>address</b>	<b>100.0.12.2 and 100.0.13.2</b>
<b>Authentication</b>	<b>Pre-share</b>

<b>Crypto ACL and Transform -set</b>	
<b>Transform-set name</b>	<b>AMS_SET</b>
<b>Encryption and Authenticaiton</b>	<b>esp-aes 256 esp-sha-hmac</b>
<b>Crypto ACL</b>	<b>192.168.2.0/24 and 192.168.3.0/24</b>

## Solution

Step 1 – IKEv2 Proposal (optional)

Step 2 – IKEv2 Policy (optional)

Step 3 – Crypto IKEv2 keyring (optional)

Step 4 – Crypto IKEv2 profile

Step 5 – Crypto ACL and IPsec Transform Set

Step 6 – Crypto Map

၁။ Lab မှတော့ default proposal, default policy, default transform-set ထွက်ပေါ် disableလုပ်ပြီးဖြစ်သင့်သလို အသစ် configure လုပ်မှာ ဖြစ်ပါတယ်။ default ထွက်ပေါ် စစ်ကြည့်ပါ။

```
R2#sh crypto ikev2 proposal
IKEv2 proposal: default
    Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
    Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
    PRF         : SHA512 SHA384 SHA256 SHA1 MD5
    DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
R2#
R2#show crypto ikev2 policy

IKEv2 policy : default
    Match fvrf : any
    Match address local : any
```

## Flex VPN

```

Proposal      : default
R2#                                                    

R2#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
    will negotiate = { Transport,   },
R2#

```

Disable လုပ်တဲ့အခါမှာလည်း default policy ကို အရင်ဖျက်ရပါတယ်။ default proposal ကို အရင်ဖျက်ရင် အသုံးပြုနေတယ်လို့ ပြပါလိမ့်မယ်။ ဖျက်ပုံကို လေ့လာကြည့်ပါ။

```

R2(config)#no crypto ikev2 proposal default
% Cannot remove as proposal is in use.
R2(config)#no crypto ikev2 policy default
R2(config)#no crypto ikev2 proposal default
R2(config)#no crypto ipsec transform-set default

```

### Step 1 – IKEv2 Proposal (optional)

<b>Step 1 – IKEv2 Proposal (optional)</b>
<pre>R2(config)#crypto ikev2 proposal AMS-PROPOSAL R2(config-ikev2-proposal)#encryption aes-cbc-256 R2(config-ikev2-proposal)#integrity sha256 R2(config-ikev2-proposal)#group 14 R2(config-ikev2-proposal)#exit</pre>

### Step 2 – IKEv2 Policy (optional)

<b>Step 2 – IKEv2 Policy (optional)</b>
<pre>R2(config)#crypto ikev2 policy AMS_POLICY IKEv2 policy MUST have atleast one complete proposal attached R2(config-ikev2-policy)#proposal AMS-PROPOSAL R2(config-ikev2-policy)#exit</pre>

### Step 3 – Crypto IKEv2 keyring (optional)

<b>Step 3 – Crypto IKEv2 keyring (optional)</b>
<pre>R2(config)#crypto ikev2 keyring AMSKEY R2(config-ikev2-keyring)#peer R3 R2(config-ikev2-keyring-peer)#address 100.0.13.2 R2(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO R2(config-ikev2-keyring-peer)#exit R2(config-ikev2-keyring)#exit</pre>

## Step 4 – Crypto IKEv2 profile

```
Step 4 - Crypto IKEv2 profile
R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any statement.
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#match identity remote address 100.0.13.2
R2(config-ikev2-profile)#keyring local AMSKEY
R2(config-ikev2-profile)#exit
```

## Step 5 – Crypto ACL and IPsec Transform Set

```
Step 5 - Crypto ACL and IPsec Transform Set
R2(config)#ip access-list extended R2_TO_R3
R2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
R2(config-ext-nacl)#exit

R2(config)#crypto ipsec transform-set AMS_SET esp-aes 256
esp-sha-hmac
R2(cfg-crypto-trans)#exit
```

## Step 6 – Crypto map

```
Step 6 - Crypto map
R2(config)#crypto map AMS_MAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
       and a valid access list have been configured.
R2(config-crypto-map)#set peer 100.0.13.2
R2(config-crypto-map)#set transform-set AMS_SET
R2(config-crypto-map)#set ikev2-profile AMS_PRO
R2(config-crypto-map)#match address R2_TO_R3
R2(config-crypto-map)#exit

R2(config)#interface ethernet 0/0
R2(config-if)#crypto map AMS_MAP
R2(config-if)#exit
*Aug 22 16:53:47.823: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

### Step 1 – IKEv2 Proposal (optional)

```
R3(config)#crypto ikev2 proposal AMS-PROPOSAL
R3(config-ikev2-proposal)#encryption aes-cbc-256
R3(config-ikev2-proposal)#integrity sha256
```

## Flex VPN

```
R3(config-ikev2-proposal)#group 14
R3(config-ikev2-proposal)#exit
```

### Step 2 - IKEv2 Policy (optional)

```
R3(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R3(config-ikev2-policy)#proposal AMS-PROPOSAL
R3(config-ikev2-policy)#exit
```

### Step 3 - Crypto IKEv2 keyring (optional)

```
R3(config)#crypto ikev2 keyring AMSKEY
R3(config-ikev2-keyring)#peer R2
R3(config-ikev2-keyring-peer)#address 100.0.12.2
R3(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit
```

### Step 4 - Crypto IKEv2 profile

```
R3(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any statement.
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#match identity remote address 100.0.12.2
R3(config-ikev2-profile)#keyring local AMSKEY
R3(config-ikev2-profile)#exit
```

### Step 5 - Crypto ACL and IPsec Transform Set

```
R3(config)#ip access-list extended R3_TO_R2
R3(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
R3(config-ext-nacl)#exit

R3(config)#crypto ipsec transform-set AMS_SET esp-aes 256
esp-sha-hmac
R3(cfg-crypto-trans)#exit
```

### Step 6 - Crypto map

```
R3(config)#crypto map AMS_MAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
R3(config-crypto-map)#set peer 100.0.12.2
R3(config-crypto-map)#set transform-set AMS_SET
R3(config-crypto-map)#set ikev2-profile AMS_PRO
R3(config-crypto-map)#match address R3_TO_R2
R3(config-crypto-map)#exit
```

## Flex VPN

```
R3(config)#interface ethernet 0/0
R3(config-if)#crypto map AMS_MAP
R3(config-if)#exit
```

### Verification

```
R2#ping 192.168.3.1 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms
R2#
```

```
R2#show crypto engine connections active
Crypto Engine Connections

      ID  Type      Algorithm          Encrypt  Decrypt LastSeqN IP-Address
      1  IPsec    AES256+SHA           0         9        9 100.0.12.2
      2  IPsec    AES256+SHA           9         0        0 100.0.12.2
  1001  IKEv2   SHA256+AES256       0         0        0 100.0.12.2
R2#
```

```
R2#show crypto ikev2 session
  IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                      Remote                  fvrf/ivrf
Status
1             100.0.12.2/500          100.0.13.2/500        none/none
READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14,
      Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/231 sec
Child sa: local selector 192.168.2.0/0 - 192.168.2.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x71E3994E/0xDAFF9E41

  IPv6 Crypto IKEv2 Session
R2#

R2#show crypto ikev2 sa
  IPv4 Crypto IKEv2 SA

Tunnel-id Local                      Remote                  fvrf/ivrf
Status
1             100.0.12.2/500          100.0.13.2/500        none/none
READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14,
      Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/287 sec

  IPv6 Crypto IKEv2 SA
R2#
```

```
R2#show crypto ipsec sa

interface: Ethernet0/0
  Crypto map tag: AMS_MAP, local addr 100.0.12.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 100.0.13.2 port 500
    PERMIT, flags={origin_is_acl,}
  #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
  #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```

### Explanation

FlexVPN site-to-site vpn ဆိတာကလည်း IKEv2 IPsec site-to-site VPN ပဲဖွစ်ပါတယ်။  
 FlexVPN ဟာ IKEv2 ကို အခြေခံပြီး အလုပ်လုပ်တာဖြစ်တဲ့အတွက် IKEv2 configuration step ကို နားလည်စေဖို့အတွက် ဒါ Lab ကို လေ့ကျင့်စေတာဖြစ်ပါတယ်။

IKEv2 configuration လုပ်တဲ့အခါ လွယ်ကူစေဖို့ IKEv2 configuration construct ကို  
 နားလည်ထားသင့်ပါတယ်။

IKEv2 Configuration	Mandatory	Smart Default	When to Configure
IKEv2 Profile	Yes	No	Always configure IKEv2 profile, as it defines the authentication method and credentials required for the negotiation
IKEv2 Proposal	No	Yes	Configure IKEv2 proposal if the default proposal does not meet the requirements
IKEv2 Keyring	No	No	
IKEv2 Global Configuration	No	No	Configure global IKEv2 parameters to apply to all peers

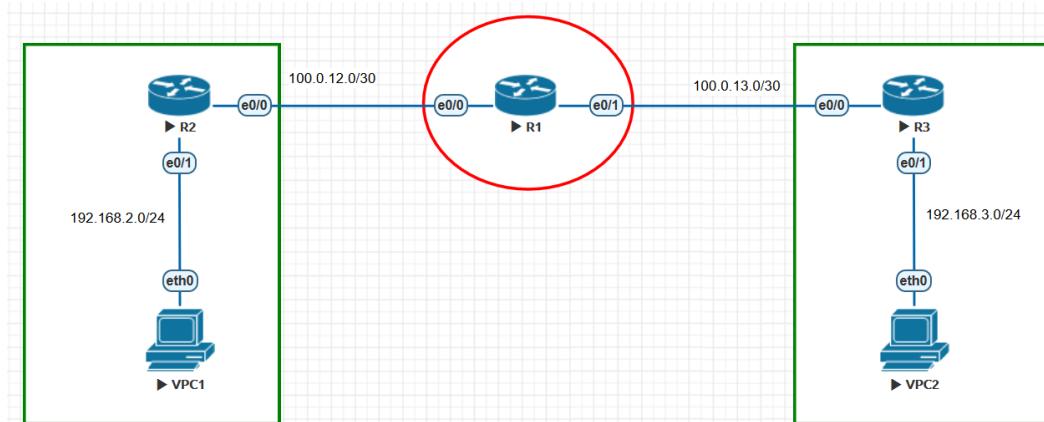
**Table 0 – 1 IKEv2 configuration constructs**

## Flex VPN

IKEv2 configuration နဲ့ပက်သက်ပြီး မဖြစ်မနေလုပ်ရမယ့်အချက်ကတော့ IKEv2 profile ဖြစ်ပါတယ်။ IKEv2 policy က IKEv2 proposal ကို define လုပ်ပါတယ်။ ကျန်တဲ့ configuration အားလုံးကိုတော့ IKEv2 profile က define လုပ်ပါတယ်။

## Lab – 2 Flex VPN with Site-to-Site with VTI

### Diagram



### Task

Configure Flexvpn Site-to-Site using following parameter:

- Use AES-CBS-256 for encryption and backup as AES-CBS-256.
- Use SHA-512 for integrity and backup as SHA-256.
- Use DH group 14.
- Use Pre-Shared key AMSCISCO for authentication.
- Use IPsec profile as IPS\_PRO

### Solution

Step 1 – IKEv2 Proposal (optional)

Step 2 – IKEv2 Policy (optional)

Step 3 – Crypto IKEv2 keyring (optional)

Step 4 – Crypto IKEv2 profile

Step 5 – Crypto IPsec Transform Set

Step 6 – Crypto IPsec Profile

## R2 configuration

အဆင့်တစ်အနေနဲ့ IKEv2 proposal configure လုပ်မှာ ဖြစ်ပါတယ်။ ရှိပြီးသား IKEv2 proposal ကို သုံးချင်ရင်လည်းရသလို့ သီးသန့် proposal configure လုပ်လည်း ရပါတယ်။ ရှိပြီးသား proposal ကို show crypto ikev2 proposal default နဲ့စစ်ကြည့်နိုင်ပါတယ်။

```
R2#show crypto ikev2 proposal default
IKEv2 proposal: default
    Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
    Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
    PRF         : SHA512 SHA384 SHA256 SHA1 MD5
    DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
R2#
```

### Step - 1 IKEv2 Proposal

```
R2(config)#crypto ikev2 proposal AMS-PROPOSAL
R2(config-ikev2-proposal)#encryption aes-cbc-256
R2(config-ikev2-proposal)#integrity sha256
R2(config-ikev2-proposal)#group 14
R2(config-ikev2-proposal)#exit
```

အဆင့်နှစ်ကတော့ IKEv2 policy configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ ဒီအဆင့်ကလည်း optional ဖြစ်တဲ့အတွက် ရှိပြီးသား default ကို သုံးချင်ရင် သုံးလို့ရပါတယ်။

```
R2#show crypto ikev2 policy default
IKEv2 policy : default
    Match fvrf : any
    Match address local : any
    Proposal     : default
R2#
```

သင့်တော်သလို့ configure လုပ်ချင်တယ်ဆိုရင်တော့ အောက်ပါအတိုင်း လုပ်ပေးရမှာ ဖြစ်ပါတယ်။

### Step - 2 IKEv2 Policy

```
R2(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R2(config-ikev2-policy)#proposal AMS_POLICY
```

အဆင့်သုံးကတော့ IKEv2 keyring configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ Key သတ်မှတ်တဲ့ အခါမှာလည်း တစ်ဘက်နဲ့တစ်ဘက် မတူလည်း ရပါတယ်။ ဥပမာ - R2 က R2AMSCISCO လို့

## Flex VPN

သုံးပြီး R3 က R3AMSCISCO လို့ မတူအောင်ထားလည်း အဆင်ပြုပါတယ်။ အခုလုပ်နေတဲ့ Lab မှာတော့ တူအောင်ထားလိုက်ပါတယ်။

### Step - 3 Crypto IKEv2 keyring

```
R2(config)#crypto ikev2 keyring AMSKEY
R2(config-ikev2-keyring)#peer R3
R2(config-ikev2-keyring-peer)#address 100.0.13.2
R2(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO

For asymmetric key
R2(config-ikev2-keyring-peer)#pre-shared-key local R2AMSCISCO
R2(config-ikev2-keyring-peer)#pre-shared-key remote R3AMSCISCO
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

အဆင့်လေးကတော့ IKEv2 profile configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ IKEv2 profile ထဲမှာ match ဖြစ်တဲ့ IKE ID သတ်မှတ်ခြင်း၊ local နဲ့ remote အတွက် authentication method သတ်မှတ်ခြင်း၊ ရှေ့မှာ configure လုပ်ခဲ့တာတွေကို reference သတ်မှတ်ခြင်း တို့ ပါဝင်ပါတယ်။

### Step - 4 Crypto IKEv2 profile

```
R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any statement.
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#match identity remote address 100.0.13.2
R2(config-ikev2-profile)#keyring local AMSKEY
R2(config-ikev2-profile)#exit
```

အဆင့်ငါးကတော့ IPsec transform set configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ ရှိပြီးသားသုံးချင်ရင်လည်း သုံးလို့ရပါတယ်။

```
R2#sh crypto ipsec transform-set default
{ esp-aes esp-sha-hmac }
  will negotiate = { Transport, },
R2#
```

သင့်တော်သလို configure လုပ်မယ်ဆိုရင်တော့ အောက်ပါအတိုင်းလုပ်ပေးရမှာ ဖြစ်ပါတယ်။

### Step 5 - Crypto IPsec Transform Set

```
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#exit
```

အဆင့်ခြေကိုကတော့ IKEv2 profile နဲ့ transform set ကို reference ပြန်လုပ်ဖို့ IPsec profile configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ IPsec profile မှာလည်း default IPsec profile ရှိပါတယ်။

```
R2#sh crypto ipsec profile default
IPSEC profile default
    Security      association      lifetime:        4608000
    kilobytes/3600 seconds
        Responder-Only (Y/N) : N
        PFS (Y/N) : N
        Mixed-mode : Disabled
        Transform sets={
            default: { esp-aes esp-sha-hmac } ,
        }
}
```

R2#

### Step - 6 Crypto IPsec profile

```
R2(config)#crypto ipsec profile IPS_PRO
R2(ipsec-profile)#set ikev2-profile AMS_PRO
R2(ipsec-profile)#set transform-set AMS_SET
R2(ipsec-profile)#exit
```

အဆင့်ခုနှစ်ကတော့ tunnel configure လုပ်ပြီး၊ IPsec profile နဲ့ protect လုပ်ပေးရှုပဲ ဖြစ်ပါတယ်။

### Step - 7 Create tunnel interface

```
R2(config)#interface Tunnel0
R2(config-if)#ip address 10.0.0.1 255.255.255.252
R2(config-if)#tunnel source Ethernet0/0
R2(config-if)#tunnel destination 100.0.13.2
R3(config-if)#tunnel mode ipsec ipv4
R2(config-if)#tunnel protection ipsec profile IPS_PRO
R2(config-if)#exit
```

အဆင့်ရှစ်ကတော့ LAN to LAN အဆက်သွယ်လုပ်နည်း static route, dynamic route run ပေးရမှာ ဖြစ်ပါတယ်။

### Step - 6 routing

```
R2(config)#router eigrp 10
R2(config-router)#network 10.0.0.1 0.0.0.0
R2(config-router)#network 192.168.2.1 0.0.0.0
R2(config-router)#exit
```

## R3 configuration

### Step - 1 Crypto IKEv2 Proposal

```
R3(config)#crypto ikev2 proposal AMS-PROPOSAL
R3(config-ikev2-proposal)#encryption aes-cbc-256
R3(config-ikev2-proposal)#integrity sha256
R3(config-ikev2-proposal)#group 14
R3(config-ikev2-proposal)#exit
```

### Step - 2 Crypto IKEv2 Policy

```
R3(config)#crypto ikev2 policy AMS_POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R3(config-ikev2-policy)#proposal AMS_POLICY
```

### Step - 3 Crypto IKEv2 keyring

```
R3(config)#crypto ikev2 keyring AMSKEY
R3(config-ikev2-keyring)#peer R2
R3(config-ikev2-keyring-peer)#address 100.0.12.2
R3(config-ikev2-keyring-peer)#pre-shared-key AMSCISCO
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit
```

### Step - 4 Crypto IKEv2 profile

```
R3(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate or match any statement.
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#match identity remote address 100.0.12.2
R3(config-ikev2-profile)#keyring local AMSKEY
R3(config-ikev2-profile)#exit
```

### Step 5 - Crypto IPsec Transform Set

```
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#exit
```

### Step - 6 Crypto IPsec profile

```
R3(config)#crypto ipsec profile IPS_PRO
R3(ipsec-profile)#set ikev2-profile AMS_PRO
R3(ipsec-profile)#set transform-set AMS_SET
R3(ipsec-profile)#exit
```

## Flex VPN

### Step - 7 Create tunnel interface

```
R3(config)#interface Tunnel0
R3(config-if)#ip address 10.0.0.2 255.255.255.252
R3(config-if)#tunnel source Ethernet0/0
R3(config-if)#tunnel destination 100.0.12.2
R3(config-if)#tunnel mode ipsec ipv4
R3(config-if)#tunnel protection ipsec profile IPS_PRO
R3(config-if)#exit
```

### Routing

```
R3(config)#router eigrp 10
R3(config-router)# network 10.0.0.2 0.0.0.0
R3(config-router)# network 192.168.3.1 0.0.0.0
R3(config-router)#exit
```

## Verification

```
R2#ping 192.168.3.1 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms
R2#
```

```
R2#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id Local           Remote           fvrf/ivrf          Status
1       100.0.12.2/500    100.0.13.2/500   none/none          READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign:
      PSK, Auth verify: PSK
      Life/Active Time: 864000/309 sec

IPv6 Crypto IKEv2 SA

R2#
```

```
R2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 100.0.12.2

protected vrf: (none)
local ident (addr/mask/prot/port): (100.0.12.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (100.0.13.2/255.255.255.255/47/0)
current_peer 100.0.13.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 109, #pkts encrypt: 109, #pkts digest: 109
  #pkts decaps: 111, #pkts decrypt: 111, #pkts verify: 111
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
```

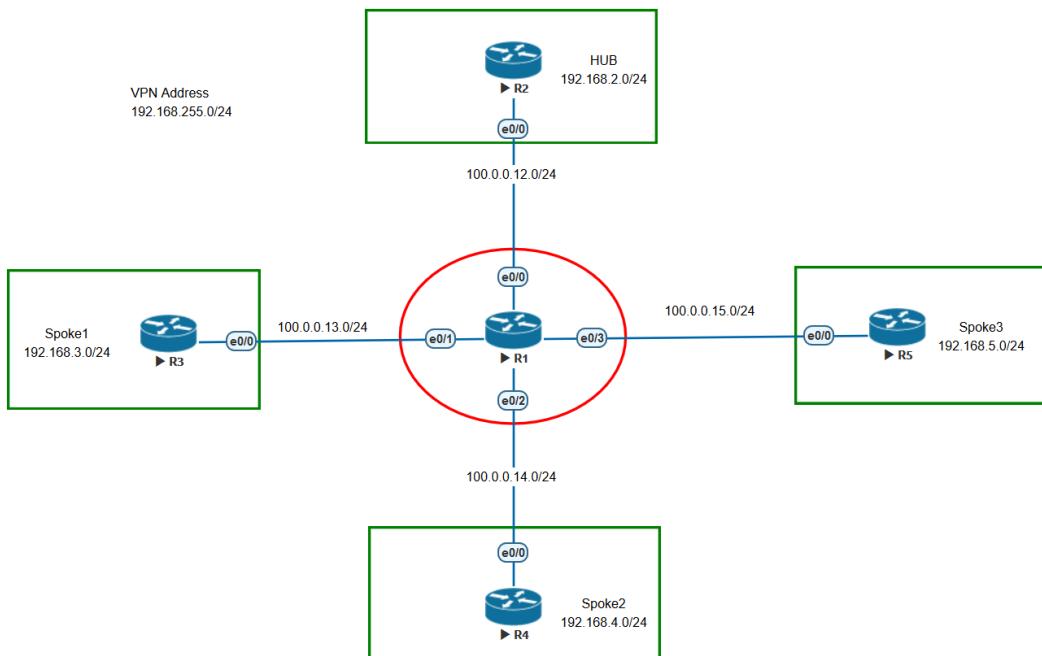
### Useful verification commands

```
R2#show run | section crypto  
R2#show crypto ikev2 profile  
R2#show crypto ikev2 proposal  
R2#show crypto engine connections active
```

အခုခိုရင် pre-shared key (PSK) ကိုသုံးပြီး FlexVPN site-to-site with tunel interface configuration တော့ အောင်မြင်သွားပါပြီ။ GRE ကိုလည်း အသုံးပြုလို့ ရပါတယ်။

## Lab – 3 Flex VPN with Hub and Spoke with ACL

### Diagram



### Lab objective

ဒဲ Lab ရဲရည်ရွယ်ချက်ကတော့ Flex VPN ကို Hub and spoke topology မှာ ဘယ်လို configures လုပ်ရတယ်ဆိုတာ နားလည်ဖို့ ရည်ရွယ်ပါတယ်။ traffic flow ကတော့ hub to spoke and spoke to spoke directly ဖြစ်ပါတယ်။

### Configuration Block

Step 1 aaa new model and aaa authorization method list

Step 2 IKEv2 authorization policy name

Step 3 Crypto IKEv2 keyring

Step 4 Crypto IKEv2 profile

Step 5 Crypto Ipsec profile

Step 6 Virtual template

## Task

- Configure Flexvpn for hub and spoke topology.

## Solution

### Hub

#### R2 (Hub)

```
R2(config)#interface Loopback0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#description LAN
R2(config-if)#interface Loopback1
R2(config-if)#description VPN Tunnel IP
R2(config-if)#ip address 192.168.255.2 255.255.255.0
R2(config-if)#interface Ethernet0/0
R2(config-if)#description R2_TO_ISP
R2(config-if)#ip address 100.0.12.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1
```

#### Step - 1

```
R2(config)#aaa new-model
R2(config)#aaa authorization network FLEX_VPN local
```

#### Step - 2

```
R2(config)#ip access-list standard HUB_ACL
R2(config-std-nacl)# permit 192.168.2.0 0.0.255.255
R2(config-std-nacl)#exit
```

```
R2(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R2(config-ikev2-author-policy)#route set interface
R2(config-ikev2-author-policy)#route set access-list HUB_ACL
R2(config-ikev2-author-policy)#exit
```

#### Step - 3

```
R2(config)#crypto ikev2 keyring AMS_KEY
R2(config-ikev2-keyring)#peer ALL_SPOKE
R2(config-ikev2-keyring-peer)#address 0.0.0.0
R2(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

#### Step - 4

```
R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
1. A local and a remote authentication method.
```

## Flex VPN

```

2. A match identity or a match certificate statement.
R2(config-ikev2-profile)#match identity remote address 0.0.0.0
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#keyring local AMS_KEY
R2(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R2(config-ikev2-profile)#virtual-template 1
R2(config-ikev2-profile)#exit

```

### Step - 5

```

R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#exit

```

```

R2(config)#crypto ipsec profile IPSEC_PRO
R2(ipsec-profile)#set transform-set AMS_SET
R2(ipsec-profile)#set ikev2-profile AMS_PRO
R2(ipsec-profile)#exit

```

### Step - 6

```

R2(config)#interface Virtual-Template1 type tunnel
R2(config-if)# ip unnumbered Loopback1
R2(config-if)# ip nhrp network-id 1
R2(config-if)# ip nhrp redirect
R2(config-if)# tunnel source Ethernet0/0
R2(config-if)# tunnel protection ipsec profile IPSEC_PRO
R2(config-if)#exit

```

## Spoke

### R3 (Spoke1)

```

R3(config)#interface Loopback0
R3(config-if)#description LAN
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#interface Loopback1
R3(config-if)#description VPN Tunnel IP
R3(config-if)#ip address 192.168.255.3 255.255.255.0
R3(config-if)#interface Ethernet0/0
R3(config-if)#description R3_TO_ISP
R3(config-if)#ip address 100.0.0.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1

```

### Step - 1

```

R3(config)#aaa new-model
R3(config)#aaa authorization network FLEX_VPN local

```

## Flex VPN

### Step - 2

```
R3(config)#ip access-list standard SPOKE_ACL
R3(config-std-nacl)#permit 192.168.3.0 0.0.0.255
R3(config-std-nacl)#exit

R3(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R3(config-ikev2-author-policy)#route set interface
R3(config-ikev2-author-policy)#route set access-list SPOKE_ACL
R3(config-ikev2-author-policy)#exit
```

### Step - 3

```
R3(config)#crypto ikev2 keyring AMS_KEY
R3(config-ikev2-keyring)#peer HUB
R3(config-ikev2-keyring-peer)#address 100.0.12.2
R3(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit
```

### Step - 4

```
R3(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate statement.
R3(config-ikev2-profile)#match identity remote address 0.0.0.0
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#keyring local AMS_KEY
R3(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R3(config-ikev2-profile)#virtual-template 1
R3(config-ikev2-profile)#exit
```

### Step - 5

```
R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R3(cfg-crypto-trans)#exit

R3(config)#crypto ipsec profile IPSEC_PRO
R3(ipsec-profile)#set transform-set AMS_SET
R3(ipsec-profile)#set ikev2-profile AMS_PRO
R3(ipsec-profile)#exit
```

### Step - 6

```
R3(config)#interface Tunnel0
R3(config-if)# ip unnumbered Loopback1
R3(config-if)# ip nhrp network-id 1
R3(config-if)# ip nhrp shortcut virtual-template 1
```

## Flex VPN

```
R3(config-if)# tunnel source Ethernet0/0
R3(config-if)# tunnel destination 100.0.12.2
R3(config-if)# tunnel protection ipsec profile IPSEC_PRO
```

### Step - 7

```
R3(config)#interface Virtual-Template1 type tunnel
R3(config-if)# ip unnumbered Loopback1
R3(config-if)# ip nhrp network-id 1
R3(config-if)# ip nhrp shortcut virtual-template 1
R3(config-if)# tunnel protection ipsec profile IPSEC_PRO
R3(config-if)#exit
```

### R4 (Spoke2)

```
R4(config)#interface Loopback0
R4(config-if)#description LAN
R4(config-if)#ip address 192.168.4.1 255.255.255.0
R4(config-if)#interface Loopback1
R4(config-if)#description VPN Tunnel IP
R4(config-if)#ip address 192.168.255.4 255.255.255.0
R4(config-if)#interface Ethernet0/0
R4(config-if)#description R4_TO_ISP
R4(config-if)#ip address 100.0.14.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#ip route 0.0.0.0 0.0.0.0 100.0.14.1
```

### Step - 1

```
R4(config)#aaa new-model
R4(config)#aaa authorization network FLEX_VPN local
```

### Step - 2

```
R4(config)#ip access-list standard SPOKE_ACL
R4(config-std-nacl)# permit 192.168.4.0 0.0.0.255
R4(config-std-nacl)#exit
R4(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R4(config-ikev2-author-policy)#route set interface
R4(config-ikev2-author-policy)#route set access-list SPOKE_ACL
R4(config-ikev2-author-policy)#exit
```

### Step - 3

```
R4(config)#crypto ikev2 keyring AMS_KEY
R4(config-ikev2-keyring)#peer HUB
R4(config-ikev2-keyring-peer)#address 100.0.12.2
R4(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R4(config-ikev2-keyring-peer)#exit
R4(config-ikev2-keyring)#exit
```

### Step - 4

```
R4(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate statement.
R4(config-ikev2-profile)#match identity remote address 0.0.0.0
R4(config-ikev2-profile)#authentication local pre-share
R4(config-ikev2-profile)#authentication remote pre-share
R4(config-ikev2-profile)#keyring local AMS_KEY
R4(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R4(config-ikev2-profile)#virtual-template 1
R4(config-ikev2-profile)#exit
```

### Step - 5

```
R4(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R4(cfg-crypto-trans)#exit

R4(config)#crypto ipsec profile IPSEC_PRO
R4(ipsec-profile)#set transform-set AMS_SET
R4(ipsec-profile)#set ikev2-profile AMS_PRO
R4(ipsec-profile)#exit
```

### Step - 6

```
R4(config)#interface Tunnel0
R4(config-if)# ip unnumbered Loopback1
R4(config-if)# ip nhrp network-id 1
R4(config-if)# ip nhrp shortcut virtual-template 1
R4(config-if)# tunnel source Ethernet0/0
R4(config-if)# tunnel destination 100.0.12.2
R4(config-if)# tunnel protection ipsec profile IPSEC_PRO
```

### Step - 7

```
R4(config)#interface Virtual-Template1 type tunnel
R4(config-if)# ip unnumbered Loopback1
R4(config-if)# ip nhrp network-id 1
R4(config-if)# ip nhrp shortcut virtual-template 1
R4(config-if)# tunnel protection ipsec profile IPSEC_PRO
R4(config-if)#exit
```

R5 ကိုလည်း R3 နဲ့ R4 အတိုင်း နည်းမျိုးပြီး configure လုပ်ပါ။

## Verification

```
R3#ping 192.168.2.1 source 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/8 ms
R3#ping 192.168.4.1 source 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
R3#
R3#traceroute 192.168.4.1 source 192.168.3.1 numeric
Type escape sequence to abort.
Tracing the route to 192.168.4.1
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.255.4 6 msec * 8 msec
R3#
```

```
R3#show ip route static | be Ga
Gateway of last resort is 100.0.13.1 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 100.0.13.1
S    192.168.0.0/16 is directly connected, Tunnel0
S    % 192.168.4.0/24 is directly connected, Virtual-Access1
      192.168.255.0/24 is variably subnetted, 4 subnets, 2 masks
S      192.168.255.2/32 is directly connected, Tunnel0
S      192.168.255.4/32 is directly connected, Virtual-Access1
R3#
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	100.0.13.3	YES	TFTP	up	up
Loopback0	192.168.3.1	YES	TFTP	up	up
Loopback1	192.168.255.3	YES	manual	up	up
Tunnel0	192.168.255.3	YES	TFTP	up	up
Virtual-Access1	192.168.255.3	YES	unset	up	up
Virtual-Template1	192.168.255.3	YES	unset	up	down

```
R3#
```

```
R3#show dmvpn | be Peer
Type:Unknown, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- -----
 1 UNKNOWN          192.168.4.1  NHRP      never     IX
Interface: Virtual-Access1, IPv4 NHRP Details
Type:Unknown, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- -----
 1 100.0.14.4       192.168.255.4    UP 00:02:23  DT2
R3#
```

## Flex VPN

```
R3#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 100.0.12.2 port 500
IKEv2 SA: local 100.0.13.3/500 remote 100.0.12.2/500 Active
IPSEC FLOW: permit 47 host 100.0.13.3 host 100.0.12.2
Active SAs: 2, origin: crypto map

Interface: Virtual-Access1
Session status: UP-ACTIVE
Peer: 100.0.14.4 port 500
IKEv2 SA: local 100.0.13.3/500 remote 100.0.14.4/500 Active
IPSEC FLOW: permit 47 host 100.0.13.3 host 100.0.14.4
Active SAs: 2, origin: crypto map

R3#
```

```
R3#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 100.0.13.3

    protected vrf: (none)
    local ident (addr/mask/prot/port): (100.0.13.3/255.255.255.255/47/0)
    remote ident (addr/mask/prot/port): (100.0.12.2/255.255.255.255/47/0)
    current_peer 100.0.12.2 port 500
        PERMIT, flags={origin_is_acl,}
        #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
        #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
```

```
R3#show crypto ikev2 authorization policy
IKEv2 Authorization Policy : default
route set interface
route accept any tag : 1 distance : 1
IKEv2 Authorization Policy : FLEX_AUTHOR
route set interface
route set acl: SPOKE_ACL
route accept any tag : 1 distance : 1
R3#
```

## Explanation

Flex VPN Hub and spoke configuration လုပ်တဲ့အခါ Hub မှာ virtual template configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။ ဘာအတွက်လဲဆိုတော့ spoke တွေနဲ့ communicate လုပ်ဖို့ ဖြစ်ပါတယ်။ နောက်တစ်ခုကတော့ DMVPN လိုပဲ nhrp enable လုပ်ဖို့ ip nhrp

network-id command နဲ့ network ID သတ်မှတ်ပေးရမှာဖြစ်ပါတယ်။ spoke to spoke တိုက်ရိုက် အဆက်သွယ်လုပ်နိုင်အောင် ip nhrp redirect ရိုက်ပေးရမှာ ဖြစ်ပါတယ်။

Hub က responder ဖြစ်ပြီး spoke တွေကတော့ initiator တွေဖြစ်ပါတယ်။ ဒါကြောင့် spoke တွေက initiate လုပ်တိုင်း virtual-template interface ကနေတဆင့် clone interface တွေဖြစ်တဲ့ virtual access interface တွေ အလိုအလျောက် create လုပ်သွားမှာ ဖြစ်ပါတယ်။

Virtual-template ပေါ်မှာ IP assign လုပ်တဲ့အခါ static IP ပေးမယ်ဆိုရင် virtual access clone မလုပ်နိုင်တော့ပါဘူး။ ဒါကြောင့် ip unnumbered ကို အသုံးပြုရပါတယ်။ ဒါကြောင့် DVTI အတွက် static IP မပေးပဲ၊ ip unnumbered ကို အသုံးပြုခဲ့တာ ဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ clone interface တွေအားလုံးဟာ virtual-template interface မှာ configure လုပ်ထားတဲ့ command တွေအားလုံးကို inherit လုပ်မှာ ဖြစ်ပါတယ်။

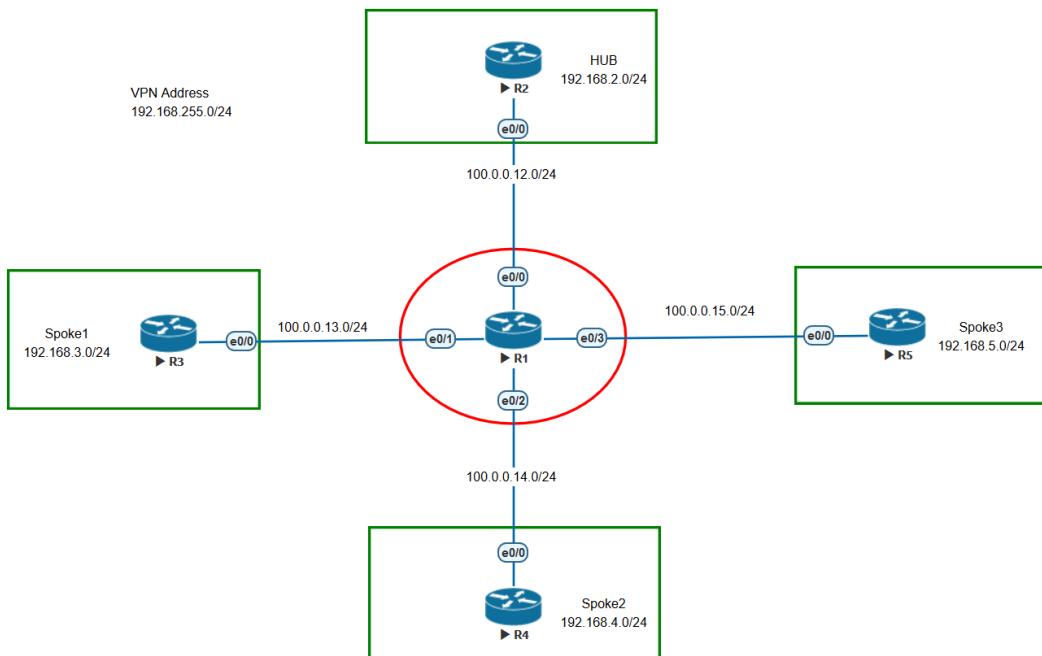
Virtual-template interface အောက်မှာ tunnel source ရှိက်ချင်ရိုက်၊ မရိုက်ချင်နေ ဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ Hub က responder ဖြစ်ပြီး spoke တွေကတော့ initiator တွေကပဲ စပြီး initiate လုပ်မှာ ဖြစ်ပါတယ်။

Spoke မှာကျတော့ tunnel interface ရယ်၊ virtual template ရယ် နှစ်ခု ဆောက်ပေးရမှာဖြစ်ပါတယ်။ tunnel interface ကတော့ Hub နဲ့ အဆက်သွယ်လုပ်ဖို့ ဖြစ်ပြီး၊ virtual template ကတော့ spoke to spoke အဆက်သွယ်လုပ်ဖို့ ဖြစ်ပါတယ်။ spoke to spoke တိုက်ရိုက်သွားနိုင်ဖို့ interface တွေရဲ့ အောက်မှာ ip nhrp shortcut ရှိက်ပေးရမှာ ဖြစ်ပါတယ်။

ACL ကိုသုံးထားတဲ့အတွက် အလိုအလျောက် static route တစ်ကြောင်း generate လုပ်ပေးပါလိမ့်မယ်။ ဒါကြောင့် dynamic routing protocol မသုံးချင်တဲ့အခါတွေမှာ အခုလို IKEv2 routing ကို အသုံးပြုလို့ရပါတယ်။ Spoke တွေကို IP ပေးတဲ့အခါ Hub ကနေ pool ဆောက်ပြီး ပေးချင်လည်းပေးလို့ရပါတယ်။ အခုလုပ်ပြုခဲ့သလို loopback ဆောက်ပြီး၊ ip unnumbered command နဲ့ IP ပေးချင်လည်း ပေးလို့ရပါတယ်။

### Lab – 4 Flex VPN with Hub and Spoke with BGP

#### Diagram



#### Lab objective

ဦး Lab ရဲ့ ရည်ရွယ်ချက်ကတော့ Flex VPN ကို Hub and spoke topology မှာ BGP နဲတဲ့ပြီး ဘယ်လို config လုပ်ရတယ်ဆိုတာ သိစေချင်တာ ဖြစ်ပါတယ်။

#### Configuration Block

- Step 1 aaa new model and aaa authorization method list
- Step 2 IKEv2 authorization policy name
- Step 3 Crypto IKEv2 keyring
- Step 4 Crypto IKEv2 profile
- Step 5 Crypto IPsec profile
- Step 6 Virtual template
- Step 7 BGP

## Task

- Configure Flexvpn for hub and spoke topology with BGP.
- Ensure that spoke to spoke communication using shortcut switching.

## Solution

### Hub

#### R2 (Hub)

```
R2(config)#interface Loopback0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#description LAN
R2(config-if)#interface Loopback1
R2(config-if)#description VPN Tunnel IP
R2(config-if)#ip address 192.168.255.2 255.255.255.0
R2(config-if)#interface Ethernet0/0
R2(config-if)#description R2_TO_ISP
R2(config-if)#ip address 100.0.12.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1
```

#### Step - 1

```
R2(config)#aaa new-model
R2(config)#aaa authorization network FLEX_VPN local
```

#### Step - 2

```
R2(config)#ip local pool SPOKES 192.168.255.4 192.168.255.254
R2(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R2(config-ikev2-author-policy)#pool SPOKES
R2(config-ikev2-author-policy)#route set interface
R2(config-ikev2-author-policy)#exit
```

#### Step - 3

```
R2(config)#crypto ikev2 keyring AMS_KEY
R2(config-ikev2-keyring)#peer ALL_SPOKE
R2(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0
R2(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

R2(config)#**crypto ikev2 profile AMS\_PRO**

IKEv2 profile MUST have:

1. A local and a remote authentication method.
2. A match identity or a match certificate statement.

R2(config-ikev2-profile)#**match identity remote address 0.0.0.0**

```
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#keyring local AMS_KEY
R2(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R2(config-ikev2-profile)#virtual-template 1
R2(config-ikev2-profile)#exit

R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#exit

R2(config)#crypto ipsec profile IPSEC_PRO
R2(ipsec-profile)#set transform-set AMS_SET
R2(ipsec-profile)#set ikev2-profile AMS_PRO
R2(ipsec-profile)#exit

R2(config)#interface Virtual-Template1 type tunnel
R2(config-if)# ip unnumbered Loopback1
R2(config-if)# ip nhrp network-id 1
R2(config-if)# ip nhrp redirect
R2(config-if)# tunnel protection ipsec profile IPSEC_PRO
R2(config-if)#exit
```

**initiator ၏ spoke ဖြစ်တဲ့အတွက်** Interface virtual-template 1 ရဲအောက်မှာ

R2(config-if)# **tunnel source Ethernet0/0** မထည့်လည်းရပါတယ်။

**Hub မှာ tunnel destination ကတေသာ လုံးဝမထည့်ရပါဘူး။**

ဒါကိုပဲ smart default ကိုသုံးပြီး အလွယ် configure လုပ်ချင်တယ်ဆိုရင်တော့  
အောက်ပါအတိုင်း လုပ်နိုင်ပါတယ်။

```
crypto ikev2 authorization policy default
crypto ikev2 profile default
crypto ipsec profile default
set ikev2-profile default
!
interface Virtual-Template1 type tunnel
    tunnel protection ipsec profile default
```

## Spoke

### R3 (Spoke1)

```
R3(config)#interface Loopback0
R3(config-if)#description LAN
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#interface Ethernet0/0
R3(config-if)#description R3_TO_ISP
R3(config-if)#ip address 100.0.13.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1
```

### Step - 1

```
R3(config)#aaa new-model
R3(config)#aaa authorization network FLEX_VPN local
```

### Step - 2

```
R3(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R3(config-ikev2-author-policy)#route set interface
R3(config-ikev2-author-policy)#exit
```

### Step - 3

```
R3(config)#crypto ikev2 keyring AMS_KEY
R3(config-ikev2-keyring)#peer FLEX-VPN
R3(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0
R3(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit
```

R3(config)#crypto ikev2 profile AMS\_PRO

IKEv2 profile MUST have:

1. A local and a remote authentication method.
2. A match identity or a match certificate statement.

```
R3(config-ikev2-profile)#match identity remote address 0.0.0.0
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#keyring local AMS_KEY
R3(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R3(config-ikev2-profile)#virtual-template 1
R3(config-ikev2-profile)#exit
```

R3(config)#crypto ipsec transform-set AMS\_SET esp-aes esp-sha-hmac

R3(cfg-crypto-trans)#exit

```
R3(config)#crypto ipsec profile IPSEC_PRO
R3(ipsec-profile)#set transform-set AMS_SET
R3(ipsec-profile)#set ikev2-profile AMS_PRO
R3(ipsec-profile)#exit

R3(config)#interface Tunnel0
R3(config-if)# ip address negotiated
R3(config-if)# ip nhrp network-id 1
R3(config-if)# ip nhrp shortcut virtual-template 1
R3(config-if)# tunnel source Ethernet0/0
R3(config-if)# tunnel destination 100.0.12.2
R3(config-if)# tunnel protection ipsec profile IPSEC_PRO

R3(config)#interface Virtual-Template1 type tunnel
R3(config-if)# ip unnumbered Tunnel0
R3(config-if)# ip nhrp network-id 1
R3(config-if)# ip nhrp shortcut virtual-template 1
R3(config-if)# tunnel protection ipsec profile IPSEC_PRO
R3(config-if)#exit
```

Tunnel 0 ကတေသ့ Hub နဲ့အဆက်သွယ်လုပ်ဖို့ဖြစ်ပါတယ်။ IP address assign လုပ်တဲ့အခါ အောက်ပါအတိုင်းလည်းလုပ်နိုင်ပါတယ်။

```
R3(config-if)#interface Loopback1
R3(config-if)#description VPN Tunnel IP
R3(config-if)#ip address 192.168.255.3 255.255.255.0
R3(config)#interface Tunnel0
R3(config-if)# ip unnumbered Loopback1
```

Virtual-template 1 ဗာ spoke to spoke communication အတွက် ဖြစ်တဲ့အတွက်

R3(config-if)# tunnel source Ethernet0/0 မထည့်လည်းရပါတယ်။

### R4 (Spoke2)

```
R4(config)#interface Loopback0
R4(config-if)#description LAN
R4(config-if)#ip address 192.168.4.1 255.255.255.0
R4(config-if)#interface Ethernet0/0
R4(config-if)#description R4_TO_ISP
R4(config-if)#ip address 100.0.14.4 255.255.255.0
R4(config-if)#no shut
```

## Flex VPN

```

R4(config-if)#exit
R4(config)#ip route 0.0.0.0 0.0.0.0 100.0.14.1

Step - 1
R4(config)#aaa new-model
R4(config)#aaa authorization network FLEX_VPN local

Step - 2
R4(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R4(config-ikev2-author-policy)#route set interface
R4(config-ikev2-author-policy)#exit

Step - 3
R4(config)#crypto ikev2 keyring AMS_KEY
R4(config-ikev2-keyring)#peer FLEX-VPN
R4(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0
R4(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R4(config-ikev2-keyring-peer)#exit
R4(config-ikev2-keyring)#exit

R4(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate statement.
R4(config-ikev2-profile)#match identity remote address 0.0.0.0
R4(config-ikev2-profile)#authentication local pre-share
R4(config-ikev2-profile)#authentication remote pre-share
R4(config-ikev2-profile)#keyring local AMS_KEY
R4(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R4(config-ikev2-profile)#virtual-template 1
R4(config-ikev2-profile)#exit

R4(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R4(cfg-crypto-trans)#exit

R4(config)#crypto ipsec profile IPSEC_PRO
R4(ipsec-profile)#set transform-set AMS_SET
R4(ipsec-profile)#set ikev2-profile AMS_PRO
R4(ipsec-profile)#exit

R4(config)#interface Tunnel0
R4(config-if)# ip address negotiated
R4(config-if)# ip nhrp network-id 1
R4(config-if)# ip nhrp shortcut virtual-template 1
R4(config-if)# tunnel source Ethernet0/0

```

## Flex VPN

```
R4(config-if)# tunnel destination 100.0.12.2
R4(config-if)# tunnel protection ipsec profile IPSEC_PRO

R4(config)#interface Virtual-Template1 type tunnel
R4(config-if)# ip unnumbered Tunnel0
R4(config-if)# ip nhrp network-id 1
R4(config-if)# ip nhrp shortcut virtual-template 1
R4(config-if)# tunnel protection ipsec profile IPSEC_PRO
R4(config-if)#exit
```

### R5 (Spoke3)

```
R5(config)#interface Loopback0
R5(config-if)#description LAN
R5(config-if)#ip address 192.168.5.1 255.255.255.0
R5(config-if)#interface Ethernet0/0
R5(config-if)#description R5_TO_ISP
R5(config-if)#ip address 100.0.15.5 255.255.255.0
R5(config-if)#no shut
R5(config-if)#exit
R5(config)#ip route 0.0.0.0 0.0.0.0 100.0.15.1

Step - 1
R5(config)#aaa new-model
R5(config)#aaa authorization network FLEX_VPN local

Step - 2
R5(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R5(config-ikev2-author-policy)#route set interface
R5(config-ikev2-author-policy)#exit

Step - 3
R5(config)#crypto ikev2 keyring AMS_KEY
R5(config-ikev2-keyring)#peer FLEX-VPN
R5(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0
R5(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R5(config-ikev2-keyring-peer)#exit
R5(config-ikev2-keyring)#exit

R5(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate statement.
R5(config-ikev2-profile)#match identity remote address 0.0.0.0
R5(config-ikev2-profile)#authentication local pre-share
R5(config-ikev2-profile)#authentication remote pre-share
```

## Flex VPN

```
R5(config-ikev2-profile)#keyring local AMS_KEY
R5(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R5(config-ikev2-profile)#virtual-template 1
R5(config-ikev2-profile)#exit

R5(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R5(cfg-crypto-trans)#exit

R5(config)#crypto ipsec profile IPSEC_PRO
R5(ipsec-profile)#set transform-set AMS_SET
R5(ipsec-profile)#set ikev2-profile AMS_PRO
R5(ipsec-profile)#exit

R5(config)#interface Tunnel0
R5(config-if)# ip address negotiated
R5(config-if)# ip nhrp network-id 1
R5(config-if)# ip nhrp shortcut virtual-template 1
R5(config-if)# tunnel source Ethernet0/0
R5(config-if)# tunnel destination 100.0.12.2
R5(config-if)# tunnel protection ipsec profile IPSEC_PRO

R5(config)#interface Virtual-Template1 type tunnel
R5(config-if)# ip unnumbered Tunnel0
R5(config-if)# ip nhrp network-id 1
R5(config-if)# ip nhrp shortcut virtual-template 1
R5(config-if)# tunnel protection ipsec profile IPSEC_PRO
R5(config-if)#exit
```

## BGP

### R2

```
R2(config)#router bgp 100
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor SPOKES peer-group
R2(config-router)#neighbor SPOKES remote-as 100
R2(config-router)#neighbor SPOKES update-source Loopback1
R2(config-router)#neighbor SPOKES route-reflector-client
R2(config-router)#network 192.168.2.0
R2(config-router)#bgp listen range 192.168.255.0/24 peer-group SPOKES
R2(config-router)#aggregate-address 192.168.0.0 255.255.0.0 summary-only
```

### R3 – R5

```

R3(config)#router bgp 100
R3(config-router)#bgp router-id 3.3.3.3
R3(config-router)#network 192.168.3.0
R3(config-router)#neighbor 192.168.255.2 remote-as 100
R3(config-router)#exit

R4(config)#router bgp 100
R4(config-router)#bgp router-id 4.4.4.4
R4(config-router)#network 192.168.4.0
R4(config-router)#neighbor 192.168.255.2 remote-as 100
R4(config-router)#exit

R5(config)#router bgp 100
R5(config-router)#bgp router-id 5.5.5.5
R5(config-router)#network 192.168.5.0
R5(config-router)#neighbor 192.168.255.2 remote-as 100
R5(config-router)#exit

```

## Verification

```

R2#show ip bgp summary | be Neighbor
Neighbor          V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.255.9  4      100    11     14      10      0      0  00:05:47      1
*192.168.255.10 4      100    11     15      10      0      0  00:05:54      1
*192.168.255.28 4      100    11     12      10      0      0  00:05:55      1
* Dynamically created based on a listen range command
Dynamically created neighbors: 3, Subnet ranges: 1

BGP peer group SPOKES listen range group members:
 192.168.255.0/24

Total dynamically created neighbors: 3/(100 max), Subnet ranges: 1

R2#

```

```

R2#show ip bgp | be Net
      Network          Next Hop            Metric LocPrf Weight Path
  *>  192.168.0.0/16  0.0.0.0                  32768  i
  s>  192.168.2.0    0.0.0.0                  0        32768  i
  s>i 192.168.3.0    192.168.255.10          0      100      0  i
  s>i 192.168.4.0    192.168.255.28          0      100      0  i
  s>i 192.168.5.0    192.168.255.9           0      100      0  i
R2#

```

```

R3#ping 192.168.2.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/6 ms

```

## Flex VPN

```
R3#ping 192.168.4.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/8 ms

R3#ping 192.168.5.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
R3#
```

```
R3#show ip route bgp | be Ga
Gateway of last resort is 100.0.13.1 to network 0.0.0.0

B      192.168.0.0/16 [200/0] via 192.168.255.2, 00:08:30
R3#
```

```
R3#trace 192.168.4.1 so 10 numeric
Type escape sequence to abort.
Tracing the route to 192.168.4.1
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.255.28 6 msec * 7 msec

R3#trace 192.168.5.1 so 10 numeric
Type escape sequence to abort.
Tracing the route to 192.168.5.1
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.255.9 6 msec * 7 msec
R3#
```

```
R3#show ip int bri | ex unas
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        100.0.13.3    YES NVRAM up           up
Loopback0          192.168.3.1    YES NVRAM up           up
Tunnel0            192.168.255.10 YES NVRAM up           up
Virtual-Access1   192.168.255.10 YES unset  up           up
Virtual-Access2   192.168.255.10 YES unset  up           up
Virtual-Access3   192.168.255.10 YES unset  up           up
Virtual-Access4   192.168.255.10 YES unset  up           up
Virtual-Template1 192.168.255.10 YES unset  up           down

R3#
```

```
R3#show dmvpn | be Peer
Type:Unknown, NHRP Peers:1,
# Ent  Peer  NBMA Addr  Peer Tunnel Add State  UpDn Tm Attrb
----- -----
2 100.0.14.4      192.168.255.28  IPSEC 00:04:34  DT1
                           192.168.255.28  IPSEC 00:03:34  DT2

Interface: Virtual-Access2, IPv4 NHRP Details
Type:Unknown, NHRP Peers:1,
```

## Flex VPN

```

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- -----
 1 100.0.14.4      192.168.255.28 IPSEC 00:03:34  DT2

Interface: Virtual-Access3, IPv4 NHRP Details
Type:Unknown, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- -----
 1 100.0.15.5      192.168.255.9   UP 00:03:07  DT2

Interface: Virtual-Access4, IPv4 NHRP Details
Type:Unknown, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- -----
 2 100.0.15.5      192.168.255.9   UP 00:04:07  DT1
                           192.168.255.9   UP 00:03:07  DT2

R3#

```

```

R3#show crypto session
Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 100.0.12.2 port 500
IKEv2 SA: local 100.0.13.3/500 remote 100.0.12.2/500
Active
IPSEC FLOW: permit 47 host 100.0.13.3 host 100.0.12.2
Active SAs: 2, origin: crypto map

Interface: Virtual-Access2
Session status: UP-ACTIVE
Peer: 100.0.14.4 port 500
IKEv2 SA: local 100.0.13.3/500 remote 100.0.14.4/500
Active
IPSEC FLOW: permit 47 host 100.0.13.3 host 100.0.14.4
Active SAs: 0, origin: crypto map
IPSEC FLOW: permit 47 host 100.0.13.3 host 100.0.14.4
Active SAs: 2, origin: crypto map

Interface: Virtual-Access4
Session status: UP-ACTIVE
Peer: 100.0.15.5 port 500
IKEv2 SA: local 100.0.13.3/500 remote 100.0.15.5/500
Active
IPSEC FLOW: permit 47 host 100.0.13.3 host 100.0.15.5
Active SAs: 2, origin: crypto map
IPSEC FLOW: permit 47 host 100.0.13.3 host 100.0.15.5

```

## Flex VPN

```
R3#show crypto ipsec sa

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 100.0.13.3

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (100.0.13.3/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (100.0.12.2/255.255.255.255/47/0)
  current_peer 100.0.12.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 648, #pkts encrypt: 648, #pkts digest: 648
    #pkts decaps: 697, #pkts decrypt: 697, #pkts verify: 697
```

```
R3#show crypto ikev2 authorization policy
IKEv2 Authorization Policy : default
  route set interface
  route accept any tag : 1 distance : 1
IKEv2 Authorization Policy : FLEX_AUTHOR
  route set interface
  route accept any tag : 1 distance : 1
R3#
```

Pool	Begin	End	Free	In use	Blocked
SPOKES	192.168.255.4	192.168.255.254	248	3	0

အကယ်၍ EIGRP သုံးချင်တယ်ဆုံးရင်တော့ အောက်ပါအတိုင်း configure လုပ်နိုင်ပါတယ်။

## EIGRP

```
R2(config)#router eigrp 10
R2(config-router)#network 192.168.2.1 0.0.0.0
R2(config-router)#network 192.168.255.2 0.0.0.0
R2(config-router)#redistribute static metric 1500 10 10 1 1500
R2(config-router)#distribute-list EIGRP_SUMMARY out
Virtual-Template1
R2(config-router)#exit

R2(config)#ip route 192.168.0.0 255.255.0.0 Null0
R2(config)#ip access-list standard EIGRP_SUMMARY
R2(config-std-nacl)#permit 192.168.0.0 0.0.255.255
R2(config-std-nacl)#exit

R3(config)#router eigrp 10
R3(config-router)#network 192.168.255.0 0.0.0.255
R3(config-router)#network 192.168.3.0 0.0.0.255
```

```
R3(config-router)#passive-interface default
R3(config-router)#no passive-interface Tunnel0

R4(config)#router eigrp 10
R4(config-router)#network 192.168.255.0 0.0.0.255
R4(config-router)#network 192.168.4.0 0.0.0.255
R4(config-router)#passive-interface default
R4(config-router)#no passive-interface Tunnel0

R5(config)#router eigrp 10
R5(config-router)#network 192.168.255.0 0.0.0.255
R5(config-router)#network 192.168.5.0 0.0.0.255
R5(config-router)#passive-interface default
R5(config-router)#no passive-interface Tunnel0
```

DMVPN network လိမ့်။ virtual-template အောက်မှ EIGRP summarization မသုံးသင့်ပါဘူး။ ဘာကြောင့်လဲဆိုတော့ virtual-access interface တွေကို replicate လုပ်တဲ့ process တွေ ရှိနေလို့ ဖြစ်ပါတယ်။ interface virtual-template ကိုလည်း access လုပ်လို့ မရတော့ပါဘူး။

```
R2(config)#int virtual-template 1 type tunnel
% Virtual-template config is locked, active vaccess present
R2(config)#interface virtual-template 1
% Virtual-template config is locked, active vaccess present
R2(config) #
```

### Explanation

ဒါ Lab ကတော့ Hub to spoke လည်း အဆက်သွယ်လုပ်ဖို့လုပ်သလို့ spoke to spoke လည်း အဆက်သွယ်လုပ်ဖို့လိုတဲ့ အခါမှာ အသုံးပြုဖို့ သင့်တော်တဲ့ design ဖြစ်ပါတယ်။

အဲဒီအတွက် SVTI, DVTI, NHRP and routing protocol တွေကို အသုံးပြုရပါတယ်။ NHRP ကို အသုံးပြုတယ်ဆိုပေမယ့်လည်း DMVPN network လို့ spoke တွေအနေနဲ့ Hub ဆီကိုသွားပြီး NHRP registration message ပို့ပြီး register လုပ်စရာမလိုသလို့ GRE multipoint interface လည်း အသုံးပြုဖို့ မလိုပါဘူး။ ဒါဆိုရင် ဘာကြောင့် NHRP ကို အသုံးပြုရသလဲလို့ မေးစရာ ရှိပါတယ်။ spoke တွေရဲ့ overlay address နဲ့ transport address ကို resolve လုပ်ပေးဖို့ NHRP ကို အသုံးပြုရတာ ဖြစ်ပါတယ်။

Hub အနေနဲ့ spoke တွေက tunnel တည်ဆောက်ဖို့အတွက် initiate လုပ်စဉ်ကတည်းက spoke တွေရဲ့ overlay IP နဲ့ transport IP ကို သိပြီးသား ဖြစ်ပါတယ်။ **show derived-config interface virtual-access 1** ဆိုပြီး ကိုယ်သိချင်တဲ့ virtual-access number ရှိက်ထည့်ပြီး စစ်ဆေးပါတယ်။

Hub configuration မှာတော့ DVTI ကို အသုံးပြုရပါတယ်။ spoke တွေက initiator အနေနဲ့ အလုပ်လုပ်ပြီး၊ Hub router ကတော့ responder အနေနဲ့ အလုပ်လုပ်မှာ ဖြစ်ပါတယ်။ ဒါကြောင့် spoke to hub tunnel တည်ဆောက်ဖို့အတွက် spoke တွေက စပြီး initiate လုပ်ရပါတယ်။ Hub အနေနဲ့ spoke တစ်ခုခြင်းစီအတွက် clone interface တွေ ဖြစ်တဲ့ virtual-access interface (VA) တွေ create လုပ်ပါတယ်။

Spoke ကတော့ hub နဲ့ tunnel တည်ဆောက်ဖို့အတွက် SVTI ကို အသုံးပြုပြီး၊ spoke to spoke tunnel တည်ဆောက်ဖို့အတွက်တော့ DVTI ကို အသုံးပြုပါတယ်။ ဒါကြောင့် Spoke မှာ interface နှစ်ခု တည်ဆောက်ပေးရပါတယ်။

Flex VPN hub and spoke tunnel ကနေဖြတ်ပြီး routing protocol run သင့်ပါတယ်။ spoke တွေအနေနဲ့လည်း တွေ့ခြား spoke နောက်မှာရှိနေတဲ့ network တွေကို routing protocol ကတဆင့် learn လုပ်နိုင်အောင် ကိုယ်သုံးနေတဲ့ routing protocol ပေါ်မှုတည့်ပြီး သင့်တော်သလို configure လုပ်ရမှာ ဖြစ်ပါတယ်။ Hub router အနေနဲ့ summarized route ကို spoke တွေဆီ ပို့ပေးရပါတယ်။

Spoke to spoke အဆက်သွယ်လုပ်ချင်တဲ့အခါ spoke တွေက traffic တွေကို hub ဆီကို ပို့လိုက်ပါတယ်။ အဲဒီလိုနဲ့ hub က ingress and egress interface (IPSec-VAs) ကို သိသွားပြီး NHRP network ID ကို share လိုက်ပြီး၊ NHRP traffic redirect လုပ်ပေးလိုက်ပါတယ်။ spoke to spoke traffic flow ကို အသေးစိတ်ကို လေ့လာကြည့်ပါ။

### Hub-Spoke tunnels

1. Spokes connect to hub, IPSec-VA created on hub for each spoke
2. IPSec-VAs for all spokes share network id

## Flex VPN

- 
- 3. Hub learns spoke networks via routing protocol over hub-spoke tunnels
  - 4. Hub advertises summarized route (via hub) to all spokes

### NHRP redirect

- 1. Spoke to spoke traffic forwarded to hub
- 2. Hub detects ingress and egress interfaces (IPSec-VAs) share NHRP network id
- 3. Hub sends NHRP traffic redirect indication to source spoke with destination spoke overlay address

### NHRP Resolution

- 1. Spoke receiving redirect initiates NHRP resolution via hub to resolve destination spoke
- 2. Hub forwards resolution request to destination spoke
- 3. Destination spoke receives resolution request, creates VA and crypto tunnel to source spoke
- 4. Destination spoke sends resolution reply over spoke-spoke direct tunnel
- 5. Destination spoke adds NHRP cache entry for source spoke

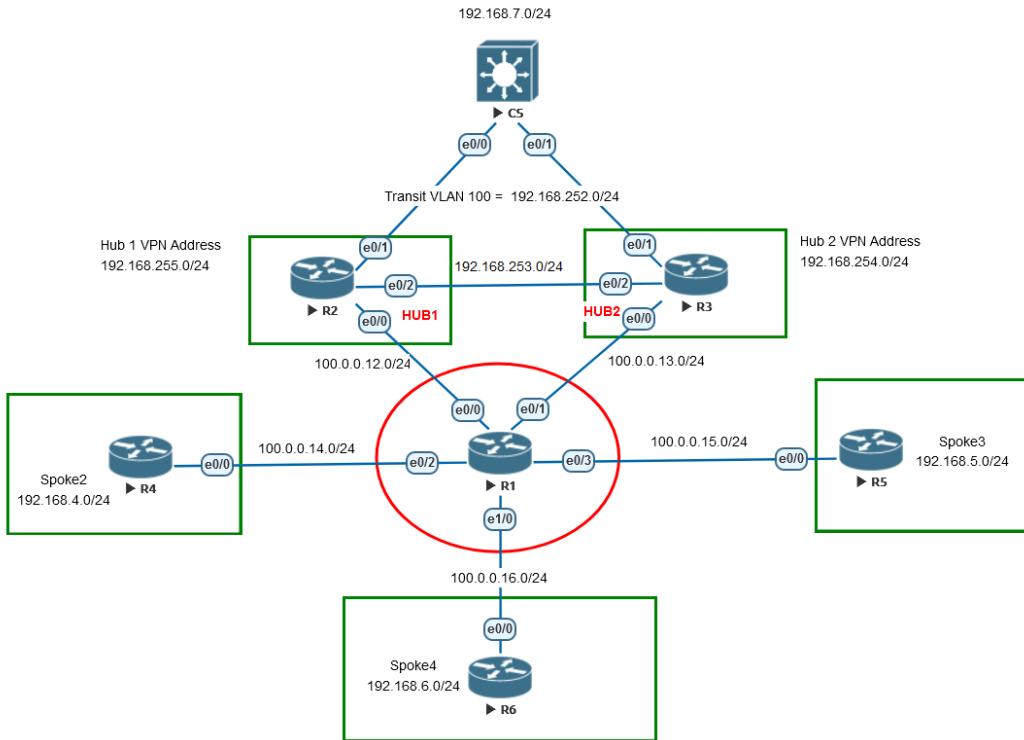
### NHRP Shortcut

- 1. Source spoke receives NHRP resolution reply
- 2. Source spoke adds NHRP cache entry and shortcut route for destination spoke

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_ike2vpn/configuration/xe-3s/sec-flex-vpn-xe-3s-book/sec-flex-spoke.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-3s/sec-flex-vpn-xe-3s-book/sec-flex-spoke.html)

## Lab – 5 Flex VPN HA Dual Hub and Dual Cloud

### Diagram



### Objective

ဗိုလ်ချုပ်လုပ်ချက်ကတေသာ့ FlexVPN HA dual hub, dual cloud configuration လုပ်ပံ့ကြသိစေချင်တာ ဖြစ်ပါတယ်။

### Task

- Configure Flex VPN for hub and spoke topology using HA Dual Hub and Dual cloud.
- Ensure that R2 is primary hub and R3 is secondary hub

Device	VPN IP (Hub and SPOKES)	(R2 and R3)	DC transit
R2	192.168. <b>255</b> .0/24	192.168.253.2/24	192.168.252.2/24
R3	192.168. <b>254</b> .0/24	192.168.253.3/24	192.168.252.3/24
R4-R6	192.168.251.X/32		

## Solution

### Hub1

#### Hub1

```
R2(config-if)#interface Loopback1
R2(config-if)#description VPN Tunnel IP
R2(config-if)#ip address 192.168.255.2 255.255.255.0
R2(config-if)#interface Ethernet0/0
R2(config-if)#description R2_TO_ISP
R2(config-if)#ip address 100.0.12.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config-if)#interface Ethernet0/1
R2(config-if)#description R2_TO_CS
R2(config-if)#ip address 192.168.252.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config-if)#interface Ethernet0/2
R2(config-if)#description R2_TO_R3
R2(config-if)#ip address 192.168.253.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit

R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1
```

#### Step - 1

```
R2(config)#aaa new-model
R2(config)#aaa authorization network FLEX_VPN local
```

#### Step - 2

```
R2(config)#ip local pool SPOKES 192.168.255.10 192.168.255.254

R2(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R2(config-ikev2-author-policy)#pool SPOKES
R2(config-ikev2-author-policy)#route set interface
R2(config-ikev2-author-policy)#exit
```

#### Step - 3

```
R2(config)#crypto ikev2 keyring AMS_KEY
R2(config-ikev2-keyring)#peer ALL_SPOKE
R2(config-ikev2-keyring-peer)#address 0.0.0.0
R2(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

```
R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
```

## Flex VPN

```

1. A local and a remote authentication method.
2. A match identity or a match certificate statement.
R2(config-ikev2-profile)#match identity remote address
0.0.0.0
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#keyring local AMS_KEY
R2(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R2(config-ikev2-profile)#virtual-template 1
R2(config-ikev2-profile)#exit

Step - 4
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#exit

R2(config)#crypto ipsec profile IPSEC_PRO
R2(ipsec-profile)#set transform-set AMS_SET
R2(ipsec-profile)#set ikev2-profile AMS_PRO
R2(ipsec-profile)#exit

R2(config)#interface Virtual-Template1 type tunnel
R2(config-if)# ip unnumbered Loopback1
R2(config-if)# ip nhrp network-id 1
R2(config-if)# ip nhrp redirect
R2(config-if)# tunnel protection ipsec profile IPSEC_PRO
R2(config-if)#exit

```

Optional အနေဖြင့် network design ပေါ်မှတည်ပြီး လိုအပ်ရင် Hub 1 and Hub2 ကြားမှာ GRE tunnel ကို အသုံးပြန်ပါတယ်။ အခုလုပ်နေတဲ့ Lab မှာတော့ R2 and R3 ကြားမှာ E0/2 ကို သုံးပြီး backdoor link ကို သုံးထားပါတယ်။ GRE tunnel မလိုပါဘူး။

```

R2(config)#interface Tunnel0
R2(config-if)#ip address 192.168.253.2 255.255.255.0
R2(config-if)#ip nhrp network-id 1
R2(config-if)#ip nhrp redirect
R2(config-if)#tunnel source Ethernet0/1
R2(config-if)#tunnel destination 192.168.252.3
R2(config-if)#exit

```

```
R3(config)#interface Tunnel0
R3(config-if)#ip address 192.168.253.3 255.255.255.0
R3(config-if)#ip nhrp network-id 1
R3(config-if)#ip nhrp redirect
R3(config-if)#tunnel source Ethernet0/1
R3(config-if)#tunnel destination 192.168.252.2
R3(config-if)#exit
```

### Hub2

#### Hub2

```
R3(config-if)#interface Loopback1
R3(config-if)#description VPN Tunnel IP
R3(config-if)#ip address 192.168.254.3 255.255.255.0
R3(config-if)#interface Ethernet0/0
R3(config-if)#description R3_TO_ISP
R3(config-if)#ip address 100.0.13.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config-if)#interface Ethernet0/1
R3(config-if)#description R3_TO_CS
R2(config-if)#ip address 192.168.252.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config-if)#interface Ethernet0/1
R3(config-if)#description R3_TO_R2
R2(config-if)#ip address 192.168.253.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
```

```
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1
```

#### Step - 1

```
R3(config)#aaa new-model
R3(config)#aaa authorization network FLEX_VPN local
```

#### Step - 2

```
R3(config)#ip local pool SPOKES 192.168.254.10 192.168.254.254
R3(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R3(config-ikev2-author-policy)#pool SPOKES
R3(config-ikev2-author-policy)#route set interface
R3(config-ikev2-author-policy)#exit
```

#### Step - 3

```
R3(config)#crypto ikev2 keyring AMS_KEY
R3(config-ikev2-keyring)#peer ALL_SPOKE
R3(config-ikev2-keyring-peer)#address 0.0.0.0
```

## Flex VPN

```
R3(config-ikev2-keyring-peer) #pre-shared-key AMSKEY
R3(config-ikev2-keyring-peer) #exit
R3(config-ikev2-keyring) #exit

R3(config) #crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate statement.
R3(config-ikev2-profile) #match identity remote address 0.0.0.0
R3(config-ikev2-profile) #authentication local pre-share
R3(config-ikev2-profile) #authentication remote pre-share
R3(config-ikev2-profile) #keyring local AMS_KEY
R3(config-ikev2-profile) #aaa authorization group psk list FLEX_VPN FLEX_AUTHOR
R3(config-ikev2-profile) #virtual-template 1
R3(config-ikev2-profile) #exit

Step - 4
R2(config) #crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R2(crypto-trans) #exit

R2(config) #crypto ipsec profile IPSEC_PRO
R2(ipsec-profile) #set transform-set AMS_SET
R2(ipsec-profile) #set ikev2-profile AMS_PRO
R2(ipsec-profile) #exit

R3(config) #interface Virtual-Template1 type tunnel
R3(config-if) # ip unnumbered Loopback1
R3(config-if) # ip nhrp network-id 1
R3(config-if) # ip nhrp redirect
R3(config-if) # tunnel protection ipsec profile IPSEC_PRO
R3(config-if) #exit
```

## Spokes

### R4

```
R4(config-if) #interface Loopback1
R4(config-if) #description VPN Tunnel IP
R4(config-if) #ip address 192.168.251.4 255.255.255.255
R4(config-if) #exit

R4(config) #interface Loopback0
R4(config-if) #description LAN
R4(config-if) #ip address 192.168.4.1 255.255.255.0
R4(config-if) #exit

R4(config-if) #interface Ethernet0/0
```

```
R4(config-if)#description R4_TO_ISP
R4(config-if)#ip address 100.0.14.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit

R4(config)#ip route 0.0.0.0 0.0.0.0 100.0.14.1

Step - 1
R4(config)#aaa new-model
R4(config)#aaa authorization network FLEX_VPN local

Step - 2
R4(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R4(config-ikev2-author-policy)#route set interface
R4(config-ikev2-author-policy)#exit

Step - 3
R4(config)#crypto ikev2 keyring AMS_KEY
R4(config-ikev2-keyring)#peer HUB
R4(config-ikev2-keyring-peer)#address 0.0.0.0
R4(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R4(config-ikev2-keyring-peer)#exit
R4(config-ikev2-keyring)#exit

R4(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate statement.
R4(config-ikev2-profile)#match identity remote address 0.0.0.0
R4(config-ikev2-profile)#authentication local pre-share
R4(config-ikev2-profile)#authentication remote pre-share
R4(config-ikev2-profile)#keyring local AMS_KEY
R4(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R4(config-ikev2-profile)#virtual-template 1
R4(config-ikev2-profile)#exit

Step - 4
R4(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R4(crypto-transform-set)#exit

R4(config)#crypto ipsec profile IPSEC_PRO
R4(ipsec-profile)#set transform-set AMS_SET
R4(ipsec-profile)#set ikev2-profile AMS_PRO
R4(ipsec-profile)#exit
```

```
R4(config)#interface Tunnel0
R4(config-if)#ip address negotiated
R4(config-if)#ip nhrp network-id 1
R4(config-if)#ip nhrp shortcut virtual-template 1
R4(config-if)#tunnel source Ethernet0/0
R4(config-if)#tunnel destination 100.0.12.2
R4(config-if)#tunnel protection ipsec profile IPSEC_PRO
R4(config-if)#exit

R4(config)#interface Tunnel1
R4(config-if)#ip address negotiated
R4(config-if)#ip nhrp network-id 1
R4(config-if)#ip nhrp shortcut virtual-template 1
R4(config-if)#tunnel source Ethernet0/0
R4(config-if)#tunnel destination 100.0.13.3
R4(config-if)#tunnel protection ipsec profile IPSEC_PRO
R4(config-if)#exit

R4(config)#interface Virtual-Template1 type tunnel
R4(config-if)# ip unnumbered Loopback1
R4(config-if)# ip nhrp network-id 1
R4(config-if)# ip nhrp shortcut virtual-template 1
R4(config-if)# tunnel protection ipsec profile IPSEC_PRO
R4(config-if)#exit
```

**R5**

```
R5(config-if)#interface Loopback1
R5(config-if)#description VPN Tunnel IP
R5(config-if)#ip address 192.168.251.5 255.255.255.255
R5(config-if)#exit

R5(config)#interface Loopback0
R5(config-if)#description LAN
R5(config-if)#ip address 192.168.5.1 255.255.255.0
R5(config-if)#exit

R5(config-if)#interface Ethernet0/0
R5(config-if)#description R5_TO_ISP
R5(config-if)#ip address 100.0.15.5 255.255.255.0
R5(config-if)#no shut
R5(config-if)#exit

R5(config)#ip route 0.0.0.0 0.0.0.0 100.0.15.1
```

## Flex VPN

```

Step - 1
R5(config)#aaa new-model
R5(config)#aaa authorization network FLEX_VPN local

Step - 2
R5(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R5(config-ikev2-author-policy)#route set interface
R5(config-ikev2-author-policy)#exit

Step - 3
R5(config)#crypto ikev2 keyring AMS_KEY
R5(config-ikev2-keyring)#peer HUB
R5(config-ikev2-keyring-peer)#address 0.0.0.0
R5(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R5(config-ikev2-keyring-peer)#exit
R5(config-ikev2-keyring)#exit

R5(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
  1. A local and a remote authentication method.
  2. A match identity or a match certificate statement.
R5(config-ikev2-profile)#match identity remote address 0.0.0.0
R5(config-ikev2-profile)#authentication local pre-share
R5(config-ikev2-profile)#authentication remote pre-share
R5(config-ikev2-profile)#keyring local AMS_KEY
R5(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R5(config-ikev2-profile)#virtual-template 1
R5(config-ikev2-profile)#exit

Step - 4
R5(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R5(cfg-crypto-trans)#exit

R5(config)#crypto ipsec profile IPSEC_PRO
R5(ipsec-profile)#set transform-set AMS_SET
R5(ipsec-profile)#set ikev2-profile AMS_PRO
R5(ipsec-profile)#exit

R5(config)#interface Tunnel0
R5(config-if)#ip address negotiated
R5(config-if)#ip nhrp network-id 1
R5(config-if)#ip nhrp shortcut virtual-template 1
R5(config-if)#tunnel source Ethernet0/0
R5(config-if)#tunnel destination 100.0.12.2
R5(config-if)#tunnel protection ipsec profile IPSEC_PRO
R5(config-if)#exit

```

## Flex VPN

```
R5(config)#interface Tunnel1
R5(config-if)#ip address negotiated
R5(config-if)#ip nhrp network-id 1
R5(config-if)#ip nhrp shortcut virtual-template 1
R5(config-if)#tunnel source Ethernet0/0
R5(config-if)#tunnel destination 100.0.0.13.3
R5(config-if)#tunnel protection ipsec profile IPSEC_PRO
R5(config-if)#exit

R5(config)#interface Virtual-Template1 type tunnel
R5(config-if)# ip unnumbered Loopback1
R5(config-if)# ip nhrp network-id 1
R5(config-if)# ip nhrp shortcut virtual-template 1
R5(config-if)# tunnel protection ipsec profile IPSEC_PRO
R5(config-if)#exit
```

### R6

```
R6(config-if)#interface Loopback1
R6(config-if)#description VPN Tunnel IP
R6(config-if)#ip address 192.168.251.6 255.255.255.255
R6(config-if)#exit
R6(config-if)#interface Loopback0
R6(config-if)#description LAN
R6(config-if)#ip address 192.168.6.1 255.255.255.0
R6(config-if)#exit

R6(config-if)#interface Ethernet0/0
R6(config-if)#description R6_TO_ISP
R6(config-if)#ip address 100.0.0.16.6 255.255.255.0
R6(config-if)#no shut
R6(config-if)#exit

R6(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.16.1

Step - 1
R6(config)#aaa new-model
R6(config)#aaa authorization network FLEX_VPN local

Step - 2
R6(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R6(config-ikev2-author-policy)#route set interface
R6(config-ikev2-author-policy)#exit

Step - 3
R6(config)#crypto ikev2 keyring AMS_KEY
R6(config-ikev2-keyring)#peer HUB
R6(config-ikev2-keyring-peer)#address 0.0.0.0
```

## Flex VPN

```

R6(config-ikev2-keyring-peer) #pre-shared-key AMSKEY
R6(config-ikev2-keyring-peer) #exit
R6(config-ikev2-keyring) #exit

R6(config) #crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
    1. A local and a remote authentication method.
    2. A match identity or a match certificate statement.
R6(config-ikev2-profile) #match identity remote address 0.0.0.0
R6(config-ikev2-profile) #authentication local pre-share
R6(config-ikev2-profile) #authentication remote pre-share
R6(config-ikev2-profile) #keyring local AMS_KEY
R6(config-ikev2-profile) #aaa authorization group psk list FLEX_VPN FLEX_AUTHOR
R6(config-ikev2-profile) #virtual-template 1
R6(config-ikev2-profile) #exit

Step - 4
R6(config) #crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R6(cfg-crypto-trans) #exit

R6(config) #crypto ipsec profile IPSEC_PRO
R6(ipsec-profile) #set transform-set AMS_SET
R6(ipsec-profile) #set ikev2-profile AMS_PRO
R6(ipsec-profile) #exit

R6(config) #interface Tunnel0
R6(config-if) #ip address negotiated
R6(config-if) #ip nhrp network-id 1
R6(config-if) #ip nhrp shortcut virtual-template 1
R6(config-if) #tunnel source Ethernet0/0
R6(config-if) #tunnel destination 100.0.12.2
R6(config-if) #tunnel protection ipsec profile IPSEC_PRO
R6(config-if) #exit

R6(config) #interface Tunnel1
R6(config-if) #ip address negotiated
R6(config-if) #ip nhrp network-id 1
R6(config-if) #ip nhrp shortcut virtual-template 1
R6(config-if) #tunnel source Ethernet0/0
R6(config-if) #tunnel destination 100.0.13.3
R6(config-if) #tunnel protection ipsec profile IPSEC_PRO
R6(config-if) #exit

R6(config) #interface Virtual-Template1 type tunnel
R6(config-if) #ip unnumbered Loopback1

```

## Flex VPN

```
R6(config-if) # ip nhrp network-id 1
R6(config-if) # ip nhrp shortcut virtual-template 1
R6(config-if) # tunnel protection ipsec profile IPSEC_PRO
R6(config-if) #exit
```

## BGP Routing

### R2

```
R2(config) #router bgp 100
R2(config-router) #bgp router-id 2.2.2.2
R2(config-router) #neighbor SPOKES peer-group
R2(config-router) #neighbor SPOKES remote-as 100
R2(config-router) #neighbor SPOKES update-source Loopback1
R2(config-router) #neighbor SPOKES route-reflector-client
R2(config-router) #bgp listen range 192.168.255.0/24 peer-group
SPOKES
R2(config-router) #neighbor 192.168.252.4 remote-as 100
R2(config-router) #neighbor 192.168.252.4 route-reflector-client
R2(config-router) #neighbor 192.168.252.4 unsuppress-map SPOKE_IP
R2(config-router) #neighbor 192.168.253.3 remote-as 100
R2(config-router) #aggregate-address 192.168.0.0 255.255.0.0
summary-only

R2(config) #ip prefix-list SPOKE_IP seq 5 permit
192.168.0.0/14 ge 24
R2(config) #route-map SPOKE_IP permit 10
R2(config-route-map) # match ip address prefix-list
SPOKE_IP
R2(config-route-map) #exit
```

### R3

```
R3(config) #router bgp 100
R3(config-router) #bgp router-id 3.3.3.3
R3(config-router) #neighbor SPOKES peer-group
R3(config-router) #neighbor SPOKES remote-as 100
R3(config-router) #neighbor SPOKES update-source Loopback1
R3(config-router) #neighbor SPOKES route-reflector-client
R3(config-router) #bgp listen range 192.168.254.0/24 peer-
group SPOKES
R3(config-router) #neighbor 192.168.252.4 remote-as 100
R3(config-router) #neighbor 192.168.252.4 route-reflector-
client
R3(config-router) #neighbor 192.168.252.4 unsuppress-map
SPOKE_IP
R3(config-router) #neighbor 192.168.253.2 remote-as 100
R3(config-router) #network 192.168.252.0
```

## Flex VPN

```
R3(config-router) #network 192.168.253.0
R3(config-router) #network 192.168.254.0
R3(config-router) #aggregate-address 192.168.0.0
255.255.0.0 summary-only
```

CS ကို BGP route တွေ advertise လုပ်တဲ့အခါ unsuppressed map ကို သုံးပြီး specific route ကို ပို့ပေးတဲ့သဘောကတော့ အကယ်၍ R1 ရဲ့ E0/0 down သွားရင် R3 က longest match ကို သုံးပြီး အနိုင်ယူနိုင်ဖို့ ဖြစ်ပါတယ်။ R2 မှာလည်း unsuppressed map သုံးထားဖို့လိုပါတယ်။ ဒါမူ R2 E0/0 link အလုပ်လုပ်နေတဲ့အခါ R3 ကို အနိုင်ယူနိုင်မှာ ဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ R2 က router-id ငယ်တဲ့အတွက် နိုင်မှာ ဖြစ်ပါတယ်။

### R4

```
R4(config) #ip prefix-list VPN_NET permit 192.168.0.0/16
R4(config) #route-map LOCAL_PRE permit 10
R4(config-route-map) #match ip address prefix-list VPN_NET
R4(config-route-map) #set local-preference 200
R4(config-route-map) #exit

R4(config) #router bgp 100
R4(config-router) #bgp router-id 4.4.4.4
R4(config-router) #neighbor 192.168.255.2 remote-as 100
R4(config-router) #neighbor 192.168.254.3 remote-as 100
R4(config-router) #neighbor 192.168.255.2 route-map LOCAL_PRE in
R4(config-router) #network 192.168.4.0
R4(config-router) #
```

### R5

```
R5(config) #ip prefix-list VPN_NET permit 192.168.0.0/16
R5(config) #route-map LOCAL_PRE permit 10
R5(config-route-map) #match ip address prefix-list VPN_NET
R5(config-route-map) #set local-preference 200
R5(config-route-map) #exit

R5(config) #router bgp 100
R5(config-router) #bgp router-id 5.5.5.5
R5(config-router) #neighbor 192.168.255.2 remote-as 100
R5(config-router) #neighbor 192.168.254.3 remote-as 100
R5(config-router) #neighbor 192.168.255.2 route-map LOCAL_PRE in
R5(config-router) #network 192.168.5.0
R5(config-router) #
```

## Flex VPN

### R6

```
R6(config)#ip prefix-list VPN_NET permit 192.168.0.0/16
R6(config)#route-map LOCAL_PRE permit 10
R6(config-route-map)#match ip address prefix-list VPN_NET
R6(config-route-map)#set local-preference 200
R6(config-route-map)#exit

R6(config)#router bgp 100
R6(config-router)#bgp router-id 6.6.6.6
R6(config-router)#neighbor 192.168.255.2 remote-as 100
R6(config-router)#neighbor 192.168.254.3 remote-as 100
R6(config-router)#neighbor 192.168.255.2 route-map LOCAL_PRE in
R6(config-router)#network 192.168.6.0
R6(config-router)#

```

### CS

```
CS(config)#vlan 100
CS(config-vlan)#name TRANSIT_VLAN
CS(config-vlan)#exit
CS(config)#int range e0/0-1
CS(config-if-range)#switchport mode access
CS(config-if-range)#switchport access vlan 100
CS(config-if-range)#exit
CS(config)#interface vlan 100
CS(config-if)#ip address 192.168.252.4 255.255.255.0
CS(config-if)#no shut
CS(config-if)#exit
CS(config)#interface loopback 0
CS(config-if)#ip add 192.168.7.1 255.255.255.0

CS(config)#router bgp 100
CS(config-router)#bgp router-id 10.10.10.10
CS(config-router)#neighbor 192.168.252.2 remote-as 100
CS(config-router)#neighbor 192.168.252.3 remote-as 100
CS(config-router)#network 192.168.7.0

```

## Verification

```
R4#ping 192.168.7.1 source 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms

```

## Flex VPN

```
R4#ping 192.168.5.1 source 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
R4#ping 192.168.6.1 source 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/7 ms
R4#
```

```
R4#traceroute 192.168.5.1 source 192.168.4.1 numeric
Type escape sequence to abort.
Tracing the route to 192.168.5.1
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.251.5 7 msec * 12 msec
R4#
```

```
R4#traceroute 192.168.6.1 source 192.168.4.1 numeric
Type escape sequence to abort.
Tracing the route to 192.168.6.1
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.251.6 7 msec * 7 msec
R4#
```

```
R4#sh ip route | in H
      o - ODR, P - periodic downloaded static route, H - NHRP, L - LISP
H    192.168.5.0/24 [250/1] via 192.168.255.11, 00:09:29, Virtual-Access2
H    192.168.6.0/24 [250/1] via 192.168.255.12, 00:09:29, Virtual-Access4
H      192.168.254.11 [250/1] via 192.168.254.11, 00:08:33, Virtual-Access2
H      192.168.255.11 [250/1] via 192.168.255.11, 00:49:38, Virtual-Access1
H      192.168.255.12 [250/1] via 192.168.255.12, 00:33:47, Virtual-Access4
R4#
```

Spoke to spoke သွားတဲ့အခါ ပထမတစ်ခေါက်တော့ Hub1 ကနေ သွားပါလိမ့်မယ်။  
နောက်အခေါက်တွေတော့ တိုက်ရှိက်သွားပါလိမ့်မယ်။

```
R2#show ip bgp summary | be Neigh
Neighbor          V      AS MsgRcvd MsgSent     TblVer  InQ OutQ Up/Down State/PfxRcd
192.168.252.4    4      100    29     28        10     0     0 00:18:57      1
192.168.253.3    4      100    0      0         1     0     0 never       Active
*192.168.255.10  4      100    27     29        10     0     0 00:20:36      1
*192.168.255.11  4      100    26     29        10     0     0 00:20:16      1
*192.168.255.12  4      100    26     30        10     0     0 00:20:07      1
* Dynamically created based on a listen range command
Dynamically created neighbors: 3, Subnet ranges: 1

BGP peergroup SPOKES listen range group members:
 192.168.255.0/24

Total dynamically created neighbors: 3/(100 max), Subnet ranges: 1
R2#
```

## Flex VPN

```
R4#show ip bgp | be Net
      Network          Next Hop            Metric LocPrf Weight
Path
 *>i 192.168.0.0/16    192.168.255.2        0     200      0 i
 * i                  192.168.254.3        0     100      0 i
 *>  192.168.4.0       0.0.0.0          0      32768   i
R4#
```

```
R4#show ip interface brief | ex unas
Interface           IP-Address      OK? Method Status      Protocol
Ethernet0/0          100.0.0.14.4    YES TFTP up          up
Loopback0             192.168.4.1     YES TFTP up          up
Loopback1             192.168.251.4    YES manual up       up
Tunnel0               192.168.255.10   YES manual up       up
Tunnel1               192.168.254.10   YES manual up       up
Virtual-Access1      192.168.251.4    YES unset up        up
Virtual-Access2      192.168.251.4    YES unset up        up
Virtual-Access4      192.168.251.4    YES unset up        up
Virtual-Template1    192.168.251.4    YES unset up        down
R4#
```

Spoke router တွေပေါ်မှာ spoke to hub communication အတွက် tunnel interface နဲ့ Spoke to spoke အဆက်သွယ်လုပ်ဖို့အတွက် virtual-template interface တည်ဆောက်ပေးရပါတယ်။ အဲဒီ virtual-template interface ကောင် clone interface ကောင်ဖြစ်တဲ့ virtual-access interface တွေ ဖြစ်လာတာဖြစ်ပါတယ်။ virtual-template1 down နေတာက်လည်း ပုံမှန်ပဲ ဖြစ်ပါတယ်။ virtual-access interface တွေ up နေဖို့လိုပါတယ်။

```
R4#show dmvpn | be Peer
Type:Unknown, NHRP Peers:1,
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
----- -----
 1 100.0.15.5      192.168.255.11 IPSEC 00:25:39   DT1

Interface: Virtual-Access2, IPv4 NHRP Details
Type:Unknown, NHRP Peers:1,
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
----- -----
 1 100.0.15.5      192.168.255.11 IPSEC 00:26:37   DT1
Interface: Virtual-Access4, IPv4 NHRP Details
Type:Unknown, NHRP Peers:1,
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
----- -----
 2 100.0.16.6      192.168.255.12      UP 00:06:33   DT1
                           192.168.255.12      UP 00:09:48   DT1
R4#
```

## Flex VPN

```
R4#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 100.0.12.2 port 500
IKEv2 SA: local 100.0.14.4/500 remote 100.0.12.2/500
Active
IPSEC FLOW: permit 47 host 100.0.14.4 host 100.0.12.2
Active SAs: 2, origin: crypto map

Interface: Virtual-Access1
Session status: UP-ACTIVE
Peer: 100.0.15.5 port 500
IKEv2 SA: local 100.0.14.4/500 remote 100.0.15.5/500
Active
IPSEC FLOW: permit 47 host 100.0.14.4 host 100.0.15.5
Active SAs: 0, origin: crypto map
IPSEC FLOW: permit 47 host 100.0.14.4 host 100.0.15.5
Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 100.0.13.3 port 500
IKEv2 SA: local 100.0.14.4/500 remote 100.0.13.3/500
Active
IPSEC FLOW: permit 47 host 100.0.14.4 host 100.0.13.3
Active SAs: 2, origin: crypto map

Interface: Virtual-Access4
Session status: UP-ACTIVE
Peer: 100.0.16.6 port 500
IKEv2 SA: local 100.0.14.4/500 remote 100.0.16.6/500
Active
IPSEC FLOW: permit 47 host 100.0.14.4 host 100.0.16.6
Active SAs: 2, origin: crypto map
R4#
```

```
R4#show crypto ipsec sa
```

```
R2#show ip local pool

Pool          Begin          End          Free  In use  Blocked
SPOKES        192.168.255.10  192.168.255.254 242      3      0
R2#
```

## Failover Test

### R2's E0/0 Fail

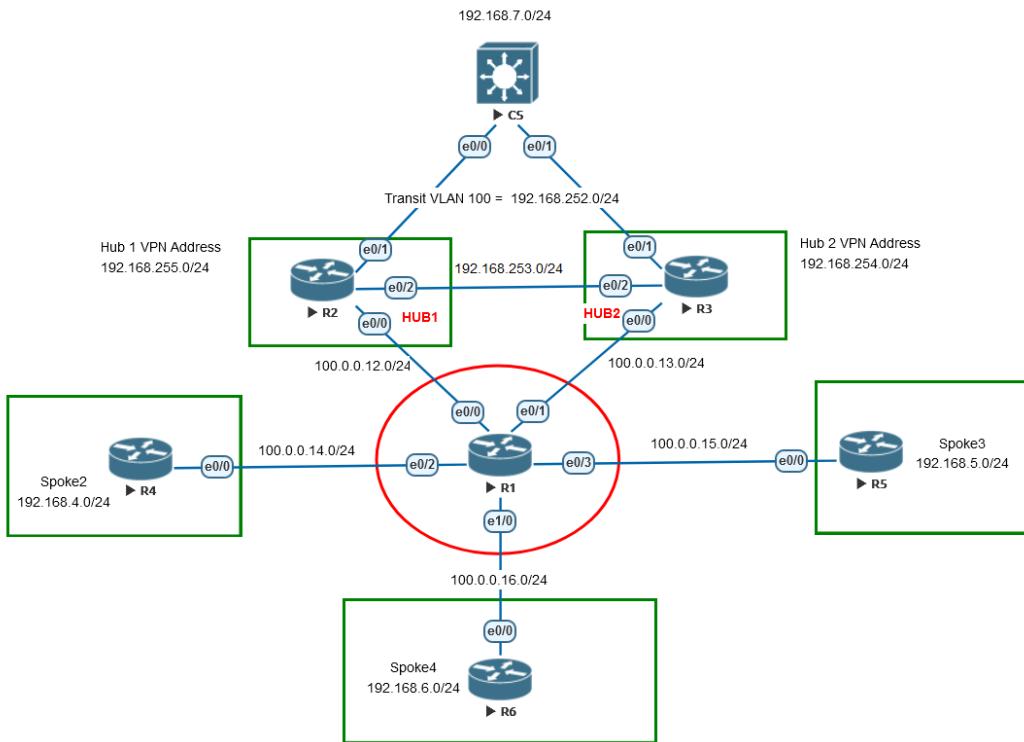
R2's E0/0 Down သွားရင် Spoke to hub communication တွေကတော့ အောက်ပါအတိုင်း  
ဖြစ်ပါတယ်။ Spoke >> R3 >> CS

### R2's E0/1 Fail

R2's E0/1 down သွားရင် Spoke to hub communication တွေကတော့ အောက်ပါအတိုင်း  
ဖြစ်ပါတယ်။ Spoke >> R2 >> R3 >> CS

## Lab – 6 Flex VPN HA Dual Hub using flex client

### Diagram



### Objective

ဒဲ Lab ရဲ့ရည်ရွယ်ချက်ကတော့ FlexVPN HA dual hub ကို flex client နဲ့ထွေပြီး configuration လုပ်ပုံကို သိစေချင်တာ ဖြစ်ပါတယ်။

### Task

- Configure Flex VPN for hub and spoke topology using HA Dual Hub with flex client.
- Ensure that R2 is primary hub and R3 is secondary hub

Device	VPN IP (Hub and SPOKES)	(R2 and R3) Backdoor	DC transit
R2	192.168.255.10/24 192.168.255.100/24	192.168.253.2/24	192.168.252.2/24
R3	192.168.255.101/24	192.168.253.3/24	192.168.252.3/24

	192.168.255.200/24		
--	--------------------	--	--

## Solution

### Hub1

#### Hub1

```
R2(config-if)#interface Loopback1
R2(config-if)#description VPN Tunnel IP
R2(config-if)#ip address 192.168.255.2 255.255.255.0
R2(config-if)#interface Ethernet0/0
R2(config-if)#description R2_TO_ISP
R2(config-if)#ip address 100.0.12.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config-if)#interface Ethernet0/1
R2(config-if)#description R2_TO_CS
R2(config-if)#ip address 192.168.252.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config-if)#interface Ethernet0/2
R2(config-if)#description R2_TO_R3
R2(config-if)#ip address 192.168.253.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit

R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1
```

#### Step - 1

```
R2(config)#aaa new-model
R2(config)#aaa authorization network FLEX_VPN local
```

#### Step - 2

```
R2(config)#ip local pool SPOKES 192.168.255.10 192.168.255.100

R2(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R2(config-ikev2-author-policy)#pool SPOKES
R2(config-ikev2-author-policy)#route set interface
R2(config-ikev2-author-policy)#exit
```

#### Step - 3

```
R2(config)#crypto ikev2 keyring AMS_KEY
R2(config-ikev2-keyring)#peer ALL_SPOKE
R2(config-ikev2-keyring-peer)#address 0.0.0.0
R2(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit
```

## Flex VPN

```
R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate statement.
R2(config-ikev2-profile)#match identity remote address
0.0.0.0
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#keyring local AMS_KEY
R2(config-ikev2-profile)#dpd 10 2 periodic
R2(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R2(config-ikev2-profile)#virtual-template 1
R2(config-ikev2-profile)#exit
```

### Step - 4

```
R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#exit
```

```
R2(config)#crypto ipsec profile IPSEC_PRO
R2(ipsec-profile)#set transform-set AMS_SET
R2(ipsec-profile)#set ikev2-profile AMS_PRO
R2(ipsec-profile)#exit
```

```
R2(config)#interface Virtual-Template1 type tunnel
R2(config-if)# ip unnumbered Loopback1
R2(config-if)# tunnel source Ethernet0/0
R2(config-if)# tunnel protection ipsec profile IPSEC_PRO
R2(config-if)#exit
```

## Hub2

### Hub2

```
R3(config-if)#interface Loopback1
R3(config-if)#description VPN Tunnel IP
R3(config-if)#ip address 192.168.255.3 255.255.255.0
R3(config-if)#interface Ethernet0/0
R3(config-if)#description R3_TO_ISP
R3(config-if)#ip address 100.0.13.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config-if)#interface Ethernet0/1
R3(config-if)#description R3_TO_CS
R2(config-if)#ip address 192.168.252.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
```

## Flex VPN

```
R3(config-if)#interface Ethernet0/1
R3(config-if)#description R3_TO_R2
R2(config-if)#ip address 192.168.253.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit

R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1

Step - 1
R3(config)#aaa new-model
R3(config)#aaa authorization network FLEX_VPN local

Step - 2
R3(config)#ip local pool SPOKES 192.168.255.101 192.168.255.254

R3(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R3(config-ikev2-author-policy)#pool SPOKES
R3(config-ikev2-author-policy)#route set interface
R3(config-ikev2-author-policy)#exit

Step - 3
R3(config)#crypto ikev2 keyring AMS_KEY
R3(config-ikev2-keyring)#peer ALL_SPOKE
R3(config-ikev2-keyring-peer)#address 0.0.0.0
R3(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit

R3(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
1. A local and a remote authentication method.
2. A match identity or a match certificate statement.
R3(config-ikev2-profile)#match identity remote address 0.0.0.0
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#keyring local AMS_KEY
R3(config-ikev2-profile)#dpd 10 2 periodic
R3(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R3(config-ikev2-profile)#virtual-template 1
R3(config-ikev2-profile)#exit

Step - 4
R3(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R3(cfg-crypto-trans)#exit
```

## Flex VPN

```
R3(config) #crypto ipsec profile IPSEC_PRO
R3(ipsec-profile) #set transform-set AMS_SET
R3(ipsec-profile) #set ikev2-profile AMS_PRO
R3(ipsec-profile) #exit

R3(config) #interface Virtual-Template1 type tunnel
R3(config-if) # ip unnumbered Loopback1
R3(config-if) # tunnel source Ethernet0/0
R3(config-if) # tunnel protection ipsec profile IPSEC_PRO
R3(config-if) #exit
```

## Spokes

R4

```
R4(config) #interface Loopback0
R4(config-if) #description LAN
R4(config-if) #ip address 192.168.4.1 255.255.255.0
R4(config-if) #exit

R4(config-if) #interface Ethernet0/0
R4(config-if) #description R4_TO_ISP
R4(config-if) #ip address 100.0.14.4 255.255.255.0
R4(config-if) #no shut
R4(config-if) #exit

R4(config) #ip route 0.0.0.0 0.0.0.0 100.0.14.1
```

### Step - 1

```
R4(config) #aaa new-model
R4(config) #aaa authorization network FLEX_VPN local
```

### Step - 2

```
R4(config) #crypto ikev2 authorization policy FLEX_AUTHOR
R4(config-ikev2-author-policy) #route set interface
R4(config-ikev2-author-policy) #exit
```

### Step - 3

```
R4(config) #crypto ikev2 keyring AMS_KEY
R4(config-ikev2-keyring) # peer HUB1
R4(config-ikev2-keyring-peer) #address 100.0.12.2
R4(config-ikev2-keyring-peer) #pre-shared-key AMSKEY
R4(config-ikev2-keyring-peer) #
R4(config-ikev2-keyring-peer) #peer HUB2
R4(config-ikev2-keyring-peer) #address 100.0.13.3
R4(config-ikev2-keyring-peer) #pre-shared-key AMSKEY
R4(config-ikev2-keyring-peer) #exit
```

```

R4(config-ikev2-keyring)#exit

R4(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
 1. A local and a remote authentication method.
 2. A match identity or a match certificate statement.
R4(config-ikev2-profile)#match identity remote address 0.0.0.0
R4(config-ikev2-profile)#authentication local pre-share
R4(config-ikev2-profile)#authentication remote pre-share
R4(config-ikev2-profile)#keyring local AMS_KEY
R4(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R4(config-ikev2-profile)#exit

R4(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R4(cfg-crypto-trans)#exit

R4(config)#crypto ipsec profile IPSEC_PRO
R4(ipsec-profile)#set transform-set AMS_SET
R4(ipsec-profile)#set ikev2-profile AMS_PRO
R4(ipsec-profile)#exit

R4(config)#interface Tunnel0
R4(config-if)#ip address negotiated
R4(config-if)#tunnel source Ethernet0/0
R4(config-if)#tunnel destination dynamic
R4(config-if)#tunnel protection ipsec profile IPSEC_PRO
R4(config-if)#exit

R4(config)#crypto ikev2 client flexvpn FLEXCLIENT
R4(config-ikev2-flexvpn)#peer 1 100.0.12.2
R4(config-ikev2-flexvpn)#peer 2 100.0.13.3
R4(config-ikev2-flexvpn)#client connect Tunnel0
R4(config-ikev2-flexvpn)#exit

```

R5 and R6 မှာလည်း R4 အတိုင်း copy and paste လုပ်ရပါပဲ။ configuration အားလုံးက အတူတူပဲ ဖြစ်ပါတယ်။

LAN to LAN အဆက်သွယ်လုပ်ဖို့အတွက် option က နှစ်ခုရှုပါတယ်။ ACL နဲ့ dynamic routing protocol ဖြစ်ပါတယ်။

## EIGRP Routing

**R2**

```
R2(config)#router eigrp 10
R2(config-router)# network 192.168.252.0
R2(config-router)# network 192.168.253.0
R2(config-router)# network 192.168.255.0
R2(config-router)#exit
```

**R3**

```
R3(config)#router eigrp 10
R3(config-router)# network 192.168.252.0
R3(config-router)# network 192.168.253.0
R3(config-router)# network 192.168.255.0
R3(config-router)#exit
```

**R4**

```
R4(config)#router eigrp 10
R4(config-router)# network 192.168.4.0
R4(config-router)# network 192.168.255.0
R4(config-router)#exit
```

**R5**

```
R5(config)#router eigrp 10
R5(config-router)# network 192.168.5.0
R5(config-router)# network 192.168.255.0
R5(config-router)#exit
```

**R6**

```
R6(config)#router eigrp 10
R6(config-router)# network 192.168.6.0
R6(config-router)# network 192.168.255.0
R6(config-router)#exit
```

**CS**

```
CS(config)#router eigrp 10
CS(config-router)# network 192.168.7.0
CS(config-router)# network 192.168.252.0
CS(config-router)#exit
```

## Verification

```
R2#show ip int brief | ex unas
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        100.0.12.2    YES NVRAM up           up
Ethernet0/1        192.168.252.2  YES NVRAM up           up
Ethernet0/2        192.168.253.2  YES NVRAM up           up
Loopback1          192.168.255.2  YES NVRAM up           up
Virtual-Access1    192.168.255.2  YES unset  up           up
Virtual-Access2    192.168.255.2  YES unset  up           up
Virtual-Access3    192.168.255.2  YES unset  up           up
Virtual-Template1 192.168.255.2  YES unset  up           down

R2#
```

## Flex VPN

```
R2#sh ip local pool

Pool           Begin          End          Free  In use  Blocked
SPOKES        192.168.255.10  192.168.255.100 88     3      0
R2#
```

```
R4#ping 192.168.7.1 source 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
```

```
R4#ping 192.168.5.1 source 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
```

```
R4#ping 192.168.6.1 source 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/7 ms
R4#
```

```
R4#traceroute 192.168.7.1 source 192.168.4.1 numeric
Type escape sequence to abort.
Tracing the route to 192.168.7.1
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.255.2 6 msec 6 msec 7 msec
 2 192.168.252.4 7 msec * 7 msec
R4#
```

```
R4#show ip route eigrp | be Ga
Gateway of last resort is 100.0.14.1 to network 0.0.0.0

D    192.168.5.0/24 [90/28288000] via 192.168.255.2, 00:03:25
D    192.168.6.0/24 [90/28288000] via 192.168.255.2, 00:03:25
D    192.168.7.0/24 [90/27033600] via 192.168.255.2, 00:02:48
D    192.168.252.0/24 [90/26905600] via 192.168.255.2, 00:02:49
D    192.168.253.0/24 [90/26905600] via 192.168.255.2, 00:03:25
    192.168.255.0/24 is variably subnetted, 5 subnets, 2 masks
D        192.168.255.0/24 [90/27008000] via 192.168.255.2, 00:03:25
D        192.168.255.14/32 [90/28160000] via 192.168.255.2, 00:03:25
D        192.168.255.16/32 [90/28160000] via 192.168.255.2, 00:03:25
R4#
```

### Failover Test

#### R2's E0/0 Fail

R2's E0/0 Down သွားရင် Spoke တွေအနေနဲ့ R3 နဲ့ GRE tunnel ဖောက်ပြီး ဆက်သွားပါလိမ့်မယ်။

#### R2's E0/1 Fail

R2's E0/1 down သွားရင် Spoke to hub communication တွေကတော့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။ Spoke >> R2 >> R3 >> CS

### Explanation

FlexVPN client and server မှာတော့ FlexVPN server ဆိုတာ IKEv2 RA server ကို ဆိုလိုတာ ဖြစ်ပါတယ်။ Remote Access and Hub-Spoke topologies တွေအတွက် IKEv2 headend functionality ကို provide လုပ်ပါတယ်။ Hub router က server ပုံစံနဲ့ အလုပ်လုပ်ပါတယ်။

Flex client configuration လုပ်တဲ့အခါ powerful peer syntax ကို အသုံးပြုနိုင်ပါတယ်။ ဆိုလိုတဲ့သဘောကတော့ ဘယ်သူက ပထမဉီးစားပေး hub ဖြစ်တယ်၊ ဘယ်သူကတော့ ဒုတိယ ဉီးစားပေးနိုင်ပါတယ်။ ဥပမာ - 100.0.12.2 က First priority hub, 100.0.13.3 က second priority hub ဖြစ်တယ်ဆိုပါစို့။ ဒါဆိုရင် အောက်ပါအတိုင်း configure လုပ်ရမှာ ဖြစ်ပါတယ်။ 10 backup gateway အတိ အသုံးပြုနိုင်တယ်လို့ ဆိုပါတယ်။

### Powerful peer syntax

```
R4(config)#crypto ikev2 client flexvpn FLEXCLIENT
R4(config-ikev2-flexvpn)#peer 1 100.0.12.2
R4(config-ikev2-flexvpn)#peer 2 100.0.13.3
R4(config-ikev2-flexvpn)#client connect Tunnel0
R4(config-ikev2-flexvpn)#exit
```

နောက်တစ်ခုကတော့ primary peer down သွားပြီး၊ ပြန်ကောင်းလာတဲ့အခါ အရင်အတိုင်း primary hub အနေနဲ့ အသုံးပြုချင်ရင် re-activation ပြန်လုပ်ပေးရပါတယ်။ အဲဒီအတွက်တော့ IP SLA and track ကို အသုံးပြုရမှာ ဖြစ်ပါတယ်။

### Re-activation on Primary Peer

```
R4(config)#ip sla 1
R4(config-ip-sla)#icmp-echo 100.0.12.2
R4(config-ip-sla-echo)#frequency 5
R4(config-ip-sla-echo)#threshold 250
R4(config-ip-sla-echo)#timeout 300
R4(config-ip-sla-echo)#exit
R4(config)#ip sla schedule 1 start-time now life forever

R4(config)#track 1 ip sla 1 reachability
R4(config-track)#delay up 1 down 1
R4(config-track)#exit

R4(config)#ip sla 2
R4(config-ip-sla)#icmp-echo 100.0.13.3
R4(config-ip-sla-echo)#frequency 5
R4(config-ip-sla-echo)#threshold 250
R4(config-ip-sla-echo)#timeout 300
R4(config-ip-sla-echo)#exit
R4(config)#ip sla schedule 2 start-time now life forever

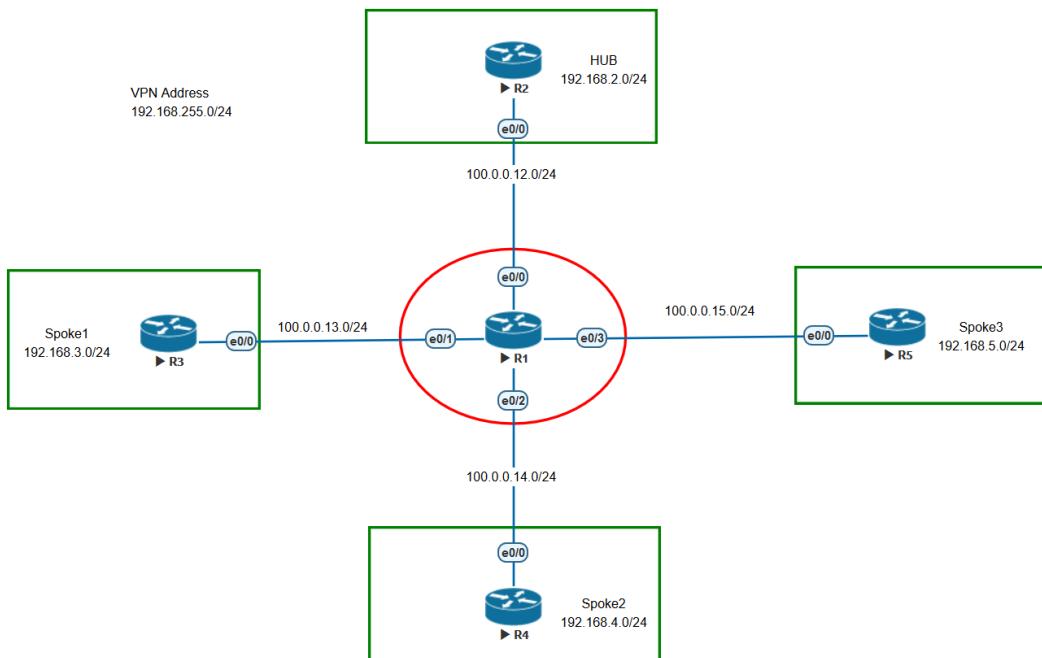
R4(config)#track 1 ip sla 2 reachability
R4(config-track)#delay up 1 down 1
R4(config-track)#exit
```

```
R4(config)#crypto ikev2 client flexvpn FLEXCLIENT
R4(config-ikev2-flexvpn)#peer 1 100.0.12.2 track 1
R4(config-ikev2-flexvpn)#peer 2 100.0.13.3 track 2
R4(config-ikev2-flexvpn)#peer reactivate
R4(config-ikev2-flexvpn)#client connect Tunnel0
```

ကျွန်ုတ္ထဲ spoke တွေမှာလည်း R4 အတိုင်းပဲ configure လုပ်ပေးရမှာ ဖြစ်ပါတယ်။

### Lab – 7 Flex VPN with Hub and Spoke with Auto mode

#### Diagram



#### Lab objective

ဦး Lab ရဲ့ ရည်ရွယ်ချက်ကတော့ Flex VPN မှာ virtual-template ကို auto mode အသုံးပြုပဲကို သိစေချင်တာ ဖြစ်ပါတယ်။ spoke တွေမှာ တချိုက် GRE interface ဖြစ်ပြီး တချိုက် IPsec VTI interface ဖြစ်နေခဲ့ရင် Hub အနေနဲ့ အားလုံးကို လက်ခံနိုင်အောင် ဖြစ်ပါတယ်။ ရှေ့မှုလုပ်ခဲ့တဲ့ Lab နဲ့ သဘောတရားခြင်းအတူတူပဲ ဖြစ်ပါတယ်။ virtual-template mode auto တစ်ခုပဲ ကွဲခြားပါတယ်။

#### Configuration Block

Step 1 aaa new model and aaa authorization method list

Step 2 IKEv2 authorization policy name

Step 3 Crypto IKEv2 keyring

Step 4 Crypto IKEv2 profile

Step 5 Crypto IPsec profile

Step 6 Virtual template

## Task

- Configure Flexvpn for hub and spoke topology with auto mode.
- Ensure that Hub can accept multiple tunnel type that come from spokes.

## Solution

### Hub

#### R2 (Hub)

```
R2(config)#interface Loopback0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#description LAN
R2(config-if)#interface Loopback1
R2(config-if)#description VPN Tunnel IP
R2(config-if)#ip address 192.168.255.2 255.255.255.0
R2(config-if)#interface Ethernet0/0
R2(config-if)#description R2_TO_ISP
R2(config-if)#ip address 100.0.12.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.12.1
```

#### Step - 1

```
R2(config)#aaa new-model
R2(config)#aaa authorization network FLEX_VPN local
```

#### Step - 2

```
R2(config)#ip local pool SPOKES 192.168.255.4 192.168.255.254
R2(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R2(config-ikev2-author-policy)#pool SPOKES
R2(config-ikev2-author-policy)#route set interface
R2(config-ikev2-author-policy)#exit
```

#### Step - 3

```
R2(config)#crypto ikev2 keyring AMS_KEY
R2(config-ikev2-keyring)#peer ALL_SPOKE
R2(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0
R2(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R2(config-ikev2-keyring-peer)#exit
R2(config-ikev2-keyring)#exit

R2(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
1. A local and a remote authentication method.
2. A match identity or a match certificate statement.
```

```
R2(config-ikev2-profile)#match identity remote address 0.0.0.0
R2(config-ikev2-profile)#authentication local pre-share
R2(config-ikev2-profile)#authentication remote pre-share
R2(config-ikev2-profile)#keyring local AMS_KEY
R2(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R2(config-ikev2-profile)#virtual-template 1 mode auto
R2(config-ikev2-profile)#exit

R2(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#exit

R2(config)#crypto ipsec profile IPSEC_PRO
R2(ipsec-profile)#set transform-set AMS_SET
R2(ipsec-profile)#set ikev2-profile AMS_PRO
R2(ipsec-profile)#exit

R2(config)#interface Virtual-Template1 type tunnel
R2(config-if)# ip unnumbered Loopback1
R2(config-if)# ip nhrp network-id 1
R2(config-if)# ip nhrp redirect
R2(config-if)# tunnel protection ipsec profile IPSEC_PRO
R2(config-if)#exit
```

အခုလုပ်နေတဲ့ Lab ဟာ ရှေ့မှာ လုပ်ခဲ့တာနဲ့ အတူတူပါပဲ။ ကွွားချက်ကတော့ virtual-template 1 mode auto တစ်ခုပဲ ကဲပါတယ်။

### Spoke

#### R3 (Spoke1)

```
R3(config)#interface Loopback0
R3(config-if)#description LAN
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#interface Ethernet0/0
R3(config-if)#description R3_TO_ISP
R3(config-if)#ip address 100.0.13.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.13.1
```

#### Step - 1

```
R3(config)#aaa new-model
R3(config)#aaa authorization network FLEX_VPN local
```

**Step - 2**

```
R3(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R3(config-ikev2-author-policy)#route set interface
R3(config-ikev2-author-policy)#exit
```

**Step - 3**

```
R3(config)#crypto ikev2 keyring AMS_KEY
R3(config-ikev2-keyring)#peer FLEX-VPN
R3(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0
R3(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R3(config-ikev2-keyring-peer)#exit
R3(config-ikev2-keyring)#exit
```

R3(config)#crypto ikev2 profile AMS\_PRO

IKEv2 profile MUST have:

1. A local and a remote authentication method.
2. A match identity or a match certificate statement.

```
R3(config-ikev2-profile)#match identity remote address 0.0.0.0
R3(config-ikev2-profile)#authentication local pre-share
R3(config-ikev2-profile)#authentication remote pre-share
R3(config-ikev2-profile)#keyring local AMS_KEY
R3(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R3(config-ikev2-profile)#virtual-template 1
R3(config-ikev2-profile)#exit
```

R3(config)#crypto ipsec transform-set AMS\_SET esp-aes esp-sha-hmac

R3(cfg-crypto-trans)#exit

R3(config)#crypto ipsec profile IPSEC\_PRO

R3(ipsec-profile)#set transform-set AMS\_SET

R3(ipsec-profile)#set ikev2-profile AMS\_PRO

R3(ipsec-profile)#exit

R3(config)#interface Tunnel0

R3(config-if)# **ip address negotiated**

R3(config-if)# ip nhrp network-id 1

R3(config-if)# ip nhrp shortcut virtual-template 1

R3(config-if)# tunnel source Ethernet0/0

R3(config-if)# tunnel destination 100.0.12.2

R3(config-if)# tunnel protection ipsec profile IPSEC\_PRO

R3(config)#interface Virtual-Template1 type tunnel

R3(config-if)# ip unnumbered Tunnel0

R3(config-if)# ip nhrp network-id 1

R3(config-if)# ip nhrp shortcut virtual-template 1

```
R3(config-if) # tunnel protection ipsec profile IPSEC_PRO
R3(config-if) #exit
```

R3 ကတော့ GRE အသုံးပြုထားပါတယ်။

### R4 (Spoke2)

```
R4(config)#interface Loopback0
R4(config-if)#description LAN
R4(config-if)#ip address 192.168.4.1 255.255.255.0
R4(config-if)#interface Ethernet0/0
R4(config-if)#description R4_TO_ISP
R4(config-if)#ip address 100.0.14.4 255.255.255.0
R4(config-if)#no shut
R4(config-if) #exit
R4(config)#ip route 0.0.0.0 0.0.0.0 100.0.14.1
```

Step - 1

```
R4(config)#aaa new-model
R4(config)#aaa authorization network FLEX_VPN local
```

Step - 2

```
R4(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R4(config-ikev2-author-policy)#route set interface
R4(config-ikev2-author-policy) #exit
```

Step - 3

```
R4(config)#crypto ikev2 keyring AMS_KEY
R4(config-ikev2-keyring) #peer FLEX-VPN
R4(config-ikev2-keyring-peer) #address 0.0.0.0 0.0.0.0
R4(config-ikev2-keyring-peer) #pre-shared-key AMSKEY
R4(config-ikev2-keyring-peer) #exit
R4(config-ikev2-keyring) #exit
```

```
R4(config)#crypto ikev2 profile AMS_PRO
```

IKEv2 profile MUST have:

1. A local and a remote authentication method.
2. A match identity or a match certificate statement.

```
R4(config-ikev2-profile) #match identity remote address 0.0.0.0
R4(config-ikev2-profile) #authentication local pre-share
R4(config-ikev2-profile) #authentication remote pre-share
R4(config-ikev2-profile) #keyring local AMS_KEY
R4(config-ikev2-profile) #aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R4(config-ikev2-profile) #virtual-template 1
```

## Flex VPN

```
R4(config-ikev2-profile)#exit

R4(config)#crypto ipsec transform-set AMS_SET esp-aes esp-sha-hmac
R4(cfg-crypto-trans)#exit

R4(config)#crypto ipsec profile IPSEC_PRO
R4(ipsec-profile)#set transform-set AMS_SET
R4(ipsec-profile)#set ikev2-profile AMS_PRO
R4(ipsec-profile)#exit

R4(config)#interface Tunnel0
R4(config-if)# ip address negotiated
R4(config-if)# ip nhrp network-id 1
R4(config-if)# ip nhrp shortcut virtual-template 1
R4(config-if)# tunnel source Ethernet0/0
R4(config-if)# tunnel destination 100.0.12.2
R4(config-if)# tunnel mode ipsec ipv4
R4(config-if)# tunnel protection ipsec profile IPSEC_PRO

R4(config)#interface Virtual-Template1 type tunnel
R4(config-if)# ip unnumbered Tunnel0
R4(config-if)# ip nhrp network-id 1
R4(config-if)# ip nhrp shortcut virtual-template 1
R4(config-if)# tunnel protection ipsec profile IPSEC_PRO
R4(config-if)#exit
```

R4 ကေတ္တာ IPsec VTI ကို အသုံးပြည်။

### R5 (Spoke3)

```
R5(config)#interface Loopback0
R5(config-if)#description LAN
R5(config-if)#ip address 192.168.5.1 255.255.255.0
R5(config-if)#interface Ethernet0/0
R5(config-if)#description R5_TO_ISP
R5(config-if)#ip address 100.0.15.5 255.255.255.0
R5(config-if)#no shut
R5(config-if)#exit
R5(config)#ip route 0.0.0.0 0.0.0.0 100.0.15.1
```

Step - 1

```
R5(config)#aaa new-model
R5(config)#aaa authorization network FLEX_VPN local
```

Step - 2

## Flex VPN

```

R5(config)#crypto ikev2 authorization policy FLEX_AUTHOR
R5(config-ikev2-author-policy)#route set interface
R5(config-ikev2-author-policy)#exit

Step - 3
R5(config)#crypto ikev2 keyring AMS_KEY
R5(config-ikev2-keyring)#peer FLEX-VPN
R5(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0
R5(config-ikev2-keyring-peer)#pre-shared-key AMSKEY
R5(config-ikev2-keyring-peer)#exit
R5(config-ikev2-keyring)#exit

R5(config)#crypto ikev2 profile AMS_PRO
IKEv2 profile MUST have:
  1. A local and a remote authentication method.
  2. A match identity or a match certificate statement.
R5(config-ikev2-profile)#match identity remote address 0.0.0.0
R5(config-ikev2-profile)#authentication local pre-share
R5(config-ikev2-profile)#authentication remote pre-share
R5(config-ikev2-profile)#keyring local AMS_KEY
R5(config-ikev2-profile)#aaa authorization group psk list
FLEX_VPN FLEX_AUTHOR
R5(config-ikev2-profile)#virtual-template 1
R5(config-ikev2-profile)#exit

R5(config)#crypto ipsec transform-set AMS_SET esp-aes esp-
sha-hmac
R5(cfg-crypto-trans)#exit

R5(config)#crypto ipsec profile IPSEC_PRO
R5(ipsec-profile)#set transform-set AMS_SET
R5(ipsec-profile)#set ikev2-profile AMS_PRO
R5(ipsec-profile)#exit

R5(config)#interface Tunnel0
R5(config-if)# ip address negotiated
R5(config-if)# ip nhrp network-id 1
R5(config-if)# ip nhrp shortcut virtual-template 1
R5(config-if)# tunnel source Ethernet0/0
R5(config-if)# tunnel destination 100.0.12.2
R5(config-if)# tunnel protection ipsec profile IPSEC_PRO
R5(config)#interface Virtual-Template1 type tunnel
R5(config-if)# ip unnumbered Tunnel0
R5(config-if)# ip nhrp network-id 1
R5(config-if)# ip nhrp shortcut virtual-template 1

```

## Flex VPN

```
R5(config-if) # tunnel protection ipsec profile IPSEC_PRO
R5(config-if) #exit
```

R5 လည်း GRE ကို အသုံးပြုထားပါတယ်။ ဒါကြောင့် R3 and R5 ဟာ တိုက်ရှုက်အဆက်သွယ်လုပ်နိုင်ပါတယ်။

## BGP

### R2

```
R2(config) #router bgp 100
R2(config-router) #bgp router-id 2.2.2.2
R2(config-router) #neighbor SPOKES peer-group
R2(config-router) #neighbor SPOKES remote-as 100
R2(config-router) #neighbor SPOKES update-source Loopback1
R2(config-router) #neighbor SPOKES route-reflector-client
R2(config-router) #network 192.168.2.0
R2(config-router) #bgp listen range 192.168.255.0/24 peer-group SPOKES
R2(config-router) #aggregate-address 192.168.0.0 255.255.0.0 summary-only
```

### R3 – R5

```
R3(config) #router bgp 100
R3(config-router) #bgp router-id 3.3.3.3
R3(config-router) #network 192.168.3.0
R3(config-router) #neighbor 192.168.255.2 remote-as 100
R3(config-router) #exit

R4(config) #router bgp 100
R4(config-router) #bgp router-id 4.4.4.4
R4(config-router) #network 192.168.4.0
R4(config-router) #neighbor 192.168.255.2 remote-as 100
R4(config-router) #exit

R5(config) #router bgp 100
R5(config-router) #bgp router-id 5.5.5.5
R5(config-router) #network 192.168.5.0
R5(config-router) #neighbor 192.168.255.2 remote-as 100
R5(config-router) #exit
```

### Verification

```
R2#show ip bgp summary | be Neighbor
Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.255.9 4      100     11     14      10      0      0 00:05:47      1
*192.168.255.10 4      100     11     15      10      0      0 00:05:54      1
*192.168.255.28 4      100     11     12      10      0      0 00:05:55      1
* Dynamically created based on a listen range command
Dynamically created neighbors: 3, Subnet ranges: 1

BGP peergroup SPOKES listen range group members:
  192.168.255.0/24

Total dynamically created neighbors: 3/(100 max), Subnet ranges: 1

R2#
```

```
R2#show ip bgp | be Net
      Network          Next Hop            Metric LocPrf Weight Path
*-> 192.168.0.0/16  0.0.0.0                  32768 i
 s-> 192.168.2.0    0.0.0.0                  32768 i
 s>i 192.168.3.0   192.168.255.10          0       100      0 i
 s>i 192.168.4.0   192.168.255.28          0       100      0 i
 s>i 192.168.5.0   192.168.255.9           0       100      0 i
R2#
```

```
R3#ping 192.168.2.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/6 ms

R3#ping 192.168.4.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/8 ms

R3#ping 192.168.5.1 so 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
R3#
```

```
R3#show ip route bgp | be Ga
Gateway of last resort is 100.0.0.13.1 to network 0.0.0.0

B      192.168.0.0/16 [200/0] via 192.168.255.2, 00:08:30
R3#
```

အကယ်၍ EIGRP သုံးချင်တယ်ဆိုရင်တော့ အောက်ပါအတိုင်း configure လုပ်နိုင်ပါတယ်။

## EIGRP

```
R2(config)#router eigrp 10
R2(config-router)#network 192.168.2.1 0.0.0.0
R2(config-router)#network 192.168.255.2 0.0.0.0
R2(config-router)#redistribute static metric 1500 10 10 1 1500
R2(config-router)#distribute-list EIGRP_SUMMARY out
Virtual-Template1
R2(config-router)#exit

R2(config)#ip route 192.168.0.0 255.255.0.0 Null0
R2(config)#ip access-list standard EIGRP_SUMMARY
R2(config-std-nacl)#permit 192.168.0.0 0.0.255.255
R2(config-std-nacl)#exit

R3(config)#router eigrp 10
R3(config-router)#network 192.168.255.0 0.0.0.255
R3(config-router)#network 192.168.3.0 0.0.0.255
R3(config-router)#passive-interface default
R3(config-router)#no passive-interface Tunnel0

R4(config)#router eigrp 10
R4(config-router)#network 192.168.255.0 0.0.0.255
R4(config-router)#network 192.168.4.0 0.0.0.255
R4(config-router)#passive-interface default
R4(config-router)#no passive-interface Tunnel0

R5(config)#router eigrp 10
R5(config-router)#network 192.168.255.0 0.0.0.255
R5(config-router)#network 192.168.5.0 0.0.0.255
R5(config-router)#passive-interface default
R5(config-router)#no passive-interface Tunnel0
```

## IPsec VPN Troubleshooting

ကျွန်တော့ အတွေ့အကြားရ IPsec VPN tunnel configures လုပ်တဲ့အခါ peer နှစ်ဖက်စလုံးမှာ တစ်ယောက်တည်း လုပ်ရတဲ့အခါမျိုးမှာတော့ လွယ်လွယ်ကူကူ အောင်အောင်မြင်မြင်နဲ့ ပြီးဆုံးလေ့ရှိပါတယ်။ ဒါပေမယ့် peer တစ်ဖက်က တဗြား SI က တာဝန်ယူရတဲ့အခါမျိုးတွေမှာတော့ အနည်းငယ် အခက်တွေရပါတယ်။

ကျွန်တော်အနေနဲ့ မှတ်မှတ်ရရ၍ Myanmar နဲ့ Dubai, Myanmar နဲ့ Singapore, Myanmar နဲ့ France IPsec tunnel configure လုပ်တုန်းက တော်တော်ကြာကြာ troubleshooting လုပ်ပြီးမှ project ပြီးသွားခဲ့ဖူးပါတယ်။ မြန်မာနိုင်ငံဘက်က ကုမ္ပဏီဘက်က ကျွန်တော်တာဝန်ယူရပါတယ်။ တဗြားဘက်အခြမ်းကတော့ တဗြား third party SI က တာဝန်ယူပါတယ်။ အဲဒီလို အခြေအနေမျိုးမှာ technology တင်မကပဲ၊ ဟိုဘက် engineer နဲ့ ဒီဘက် engineer မတူညီတဲ့ SI နှစ်ခု error ဖြေရှင်းဖို့ လူအချင်းချင်းပါ ညီးနှင့်မှတွေ လုပ်ရတတ်ပါတယ်။ error တက်တဲ့အခါ သူ့ကြောင့်၊ ကိုယ့်ကြောင့် အငြင်းပွားနေမယ့်အစား technology ကို ပိုင်ပိုင်နိုင်နိုင်သိထားပြီး အထောက်ထားနဲ့ ပြောဆို ညီးနှင့်တတ်ဖို့ လိုပါတယ်။

troubleshooting လုပ်တယ်ဆိုတာ ကလည်း စနစ်တကျ လေ့လာထားတဲ့ theory နဲ့ အတွေ့ကြံကို ပေါင်းစပ်ပြီး ပြဿနာကို ဖြေရှင်းရတာ ဖြစ်ပါတယ်။

troubleshooting လုပ်တဲ့အခါ အသုံးများဆုံးကတော့ verification command တွေဖြစ်တဲ့ show command တွေနဲ့ debug command တွေ ဖြစ်ပါတယ်။ show command တွေနဲ့ debug command တွေ သုံးတတ်ဖို့ အလွန်အင်မတန်မှ အရေးကြီးပါတယ်။ ဒါကြောင့် IPsec tunnel implementation လုပ်တဲ့အခါ တွေ့ရတတ်တဲ့ error များနဲ့ troubleshooting step တွေကို လေ့လာကြည့်ရအောင်။

နံပါတ်တစ်ကတော့ Phase1 issue လား၊ Phase 2 issue လား ရှင်းရှင်းလင်းလင်း သိအောင် လုပ်ပါ။ Phase 1 မအောင်မြင်ပဲနဲ့ phase 2 ဆိုတာ မဖြစ်နိုင်ပါဘူး။ phase tunnel up ရဲလား အရင် စစ်ပါ။

**Phase 1 ဘာကြောင့် မအောင်မြင်တတ်သလဲ?**

Phase 1 မှာ အသုံးပြုတဲ့ Crypto algorithm တွေ peer နှစ်ခု လွှဲနေတာတို့! UDP port 500 ကို block လုပ်ထားတာတို့ pre-shared key မှားနေတာတို့ဖြစ်တတ်ပါတယ်။ phase 2 မှာလည်း transform set မှာ နှစ်ဘက် အသုံးပြုမယ့် encryption method and authentication method တွေ တူမတူ စစ်ရပါတယ်။ Access-control list (ACL) တွေ စစ်ရပါတယ်။ crypto map အောက်မှာ peer မှန်၊ မမှန် စစ်ရပါတယ်။

phase 1 အတွက် အသုံးပြုများတဲ့ command တွေကို လေလာကြည့်ပါ။

### Show crypto isakmp sa

ဒဲ command ကတော့ peer နှစ်ခုကြားမှာ တည်ဆောက်ထားတဲ့ Internet Security Association Management Protocol (ISAKMP) security associations (SAs) ကိုဖော်ပြပေးတာ ဖြစ်ပါတယ်။ Phase 1 မှာ အဆင့်တစ် negotiation, အဆင့်နှစ် key exchange, အဆင့်သုံး authentication ဖြစ်တဲ့အတွက် နောက်ဆုံးအဆင့် authentication successful ဖြစ်တယ်ဆိုရင် phase 1 အောင်မြင်ပါပြီ။

```
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id status
100.0.12.2   100.0.13.2   QM_IDLE   1002 ACTIVE
100.0.13.2   100.0.12.2   QM_IDLE   1003 ACTIVE

IPv6 Crypto ISAKMP SA
R2#
```

### show crypto ikev2 sa

ဒဲ command လည်း IKEv2 sa ကို စစ်တဲ့ command ဖြစ်ပါတယ်။

Show crypto session

ဒဲ command ကတော့ active ဖြစ်နေတဲ့ crypto session တွေကို စစ်တဲ့ command ဖြစ်ပါတယ်။

## IPsec VPN

Phase 1 အောင်မြင်တယ်ဆိုရင်တော့ phase 2 ကို ဆက်စစ်ကြည့်ရမှာ ဖြစ်ပါတယ်။ အသုံးများတဲ့ show command ကတော့ **show crypto ipsec sa** ဖြစ်ပါတယ်။ encryption packet and decryption packet တွေကို စစ်ကြည့်ရမှာ ဖြစ်ပါတယ်။ phase 2 စစ်တဲ့ command တစ်ခုကတော့ **show crypto engine connection active** ဖြစ်ပါတယ်။

**show crypto engine connection active** ကတော့ phase 2 SA နဲ့ ပို့ထားတဲ့ traffic ကို စစ်နိုင်ပါတယ်။

phase 1 နဲ့ phase 2 မှာ အသုံးများတဲ့ debug command တွေကတော့ debug crypto isakmp, debug crypt engine နဲ့ debug crypto ipsec တို့ဖြစ်ပါတယ်။

IKEv2 မှာ အသုံးများတဲ့ command တွေကတော့ show crypto ikev2 sa detailed, show crypto ipsec sa, show crypto session, deb crypto ikev2 packet, deb crypto ikev2 internal တို့ဖြစ်ပါတယ်။

## နိဂုံး

အချလောက်ဆိုရင် IPsec VPN solution ကို နားလည်သဘောပေါက်ပြီး၊ Lab တွေအားလုံးကိုလည်း စနစ်တကျ လေ့ကျင့်ပြီးသွားပြီလို့ ယုံကြည်ပါတယ်။ IPsec VPN ဟာ Enterprise network မှာ ရုံးအားလုံးနီးပါး အသုံးပြုကြတဲ့အတွက် သိသင့်သိထိက်တဲ့ technology တစ်ခု ဖြစ်ပါတယ်။ ဒါကြောင့် ဒီစာအုပ်ကနေ တစ်စုတရာ အကျိုးရှိမယ်ဆိုရင် ရေးရကျိုးနှပ်ပါပြီ။ ဒီစာအုပ်ရေးတဲ့အခါ အဓိက reference လုပ်ထားတဲ့ resource တွေကိုလည်း မူရင်းအတိုင်း လေ့လာလိုသူများအတွက် ဖော်ပြုပေးလိုက်ပါတယ်။

Ref:

BRKSEC-1050 and Cisco Press IKEv2 VPN book

<https://www.cisco.com/c/en/us/support/docs/security/flexvpn/115782-flexvpn-site-to-site-00.html>

တိုးတက်၊ အောင်မြင်၊ ပျော်ရွင်၊ ပြိုမ်းချမ်းကြပါစေ။

အောင်နိုင်မှုး (AMS)