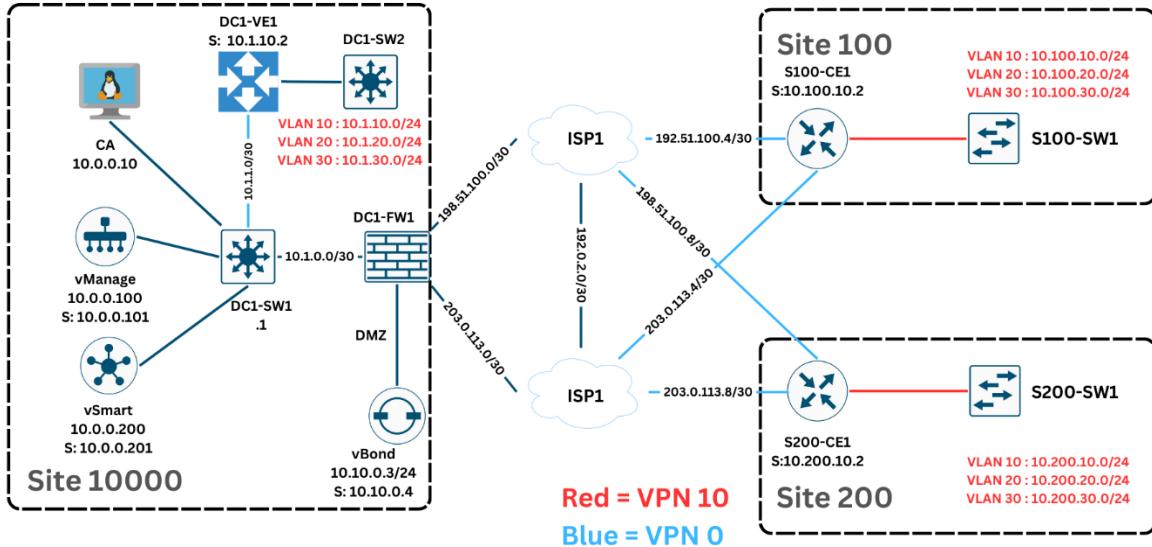


Cisco SD-WAN: Basic Configuration Lab

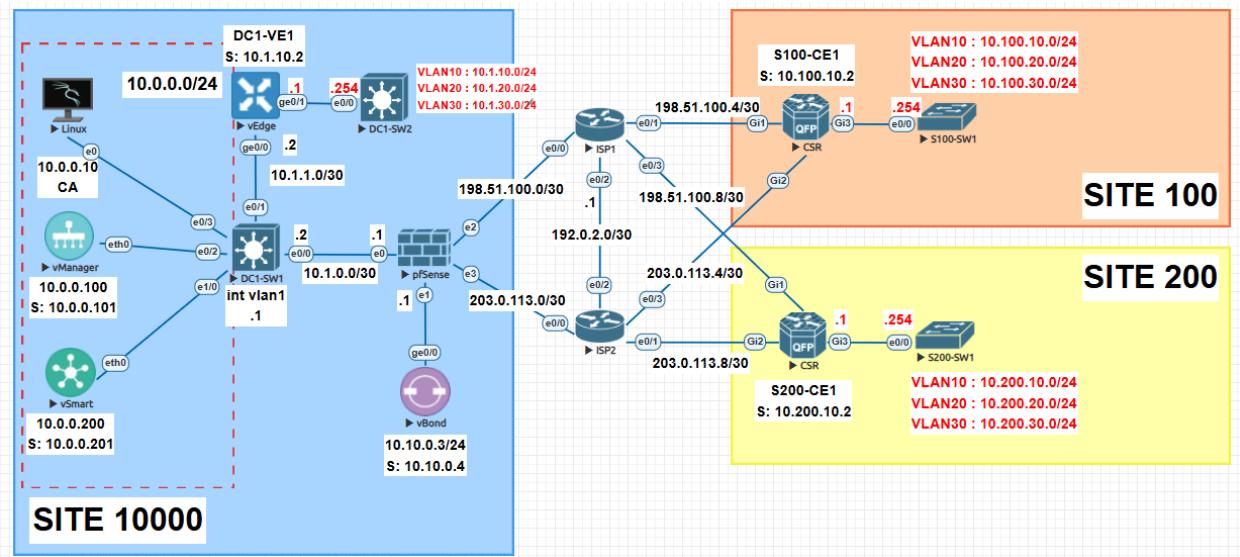


อุปกรณ์

Image

Kali Linux	linux-kali-2023
L3 & L2 Switch	i86bi_linux_l2-adventerprisek9-ms.SSA.high_iron_20190423
vManage (vtmgmt)	vtmgmt-19.2.0
vSmart (vtsmart)	vtsmart-19.2.0
vBond (vtbond)	vtbond-19.2.0
vEdge (vtedge)	csr1000vng-ucmk9.16.12.1b-sdwan
Firewall	pfSense

Note : Initial Lab Setup on Page 20



Planning sites and system IDs

ใน Cisco SD-WAN เป็นขั้นตอนสำคัญที่ช่วยให้การบริหารจัดการระบบมีความเป็นระเบียบและลดความซับซ้อนในการกำหนดค่าเครือข่าย Site ID เป็นหมายเลข 32 บิตที่ใช้ระบุสถานที่ตั้งของอุปกรณ์ SD-WAN แต่ละตัวภายในองค์กร โดยแต่ละ Site ID จะต้องไม่ซ้ำกันเพื่อให้สามารถระบุอุปกรณ์ใน Control Plane ได้อย่างชัดเจน

System ID เป็นหมายเลข 32 บิตในรูปแบบ dotted decimal ซึ่งต้องอยู่ในช่วงของ valid unicast IP address แม้ว่าค่า System ID จะมีลักษณะคล้ายกับ loopback address หรือ router ID ของโพรโทคอลเราเตอร์ แต่ก็มีข้อกำหนดที่สำคัญคือค่านี้จะต้องไม่ถูกกำหนดให้กับอินเทอร์เฟซใด ๆ บนอุปกรณ์ SD-WAN และต้องมีความเป็นเอกลักษณ์ภายใน SD-WAN fabric

สำหรับแนวทางการกำหนดค่า System ID หนึ่งในวิธีที่นิยมใช้กันคือการเลือกหมายเลขที่อยู่ภายใต้ช่วงของ IP subnet ที่อุปกรณ์ SD-WAN ใช้งานอยู่ เช่น หากอุปกรณ์ cEdge S100-CE1 มี IP address ของอินเทอร์เฟซเป็น 10.100.10.1 ก็สามารถกำหนดค่า System ID ให้เป็น 10.100.10.2 ได้ วิธีนี้ช่วยให้สามารถจดจำและจัดการค่าต่าง ๆ ได้ง่ายขึ้น เนื่องจาก System ID และ IP address ของอินเทอร์เฟซมีความสัมพันธ์กันโดยตรง การกำหนดค่าที่เป็นระเบียบและมีรูปแบบที่แน่นอนจะช่วยให้การบริหารจัดการระบบ SD-WAN เป็นไปอย่างมีประสิทธิภาพ ลดความสับสน และช่วยให้สามารถขยายระบบได้ง่ายขึ้นในอนาคต

Planning VPNs

ภายใน Cisco SD-WAN fabric แนวคิดของ VPNs มีความคล้ายคลึงกับ VRFs ในระบบเราเตอร์แบบดั้งเดิม โดย VPN แต่ละตัวจะถูกแยกออกจากกันตามค่าเริ่มต้น อุปกรณ์ที่อยู่ภายใต้ VPN หนึ่งจะไม่สามารถสื่อสารกับอุปกรณ์ที่อยู่ใน VPN อื่นได้ เว้นแต่ว่าจะมีการกำหนด policy เพื่อนำมาตัดต่อ กันได้

ลักษณะการทำงานของ VPNs ใน SD-WAN fabric คือ ทุกอินเทอร์เฟซหรือชั้บอินเทอร์เฟซสามารถเป็นสมาชิกของ VPN ได้เพียงตัวเดียวเท่านั้น หากไม่มีการกำหนดนโยบายเพิ่มเติม อุปกรณ์ทั้งหมดที่อยู่ภายใต้ VPN เดียวกันจะสามารถสื่อสารกันได้โดยอัตโนมัติ และมีรูปแบบ full-mesh topology หรือการเชื่อมต่อแบบ any-to-any ซึ่งเป็นค่าเริ่มต้นของระบบ

อย่างไรก็ตาม สามารถกำหนด policy เพื่อเปลี่ยนรูปแบบการเชื่อมต่อของแต่ละ VPN ได้ตามความต้องการ ภายใน SD-WAN fabric เดียว กัน อาจมี VPN หนึ่งที่ใช้ full-mesh topology อีก VPN ที่ใช้ hub-and-spoke และอีก VPN ที่มีการกำหนด partial-mesh เพื่อจำกัดการเชื่อมต่อระหว่างบังไช์ต่อกัน วิธีนี้ช่วยให้สามารถออกแบบเครือข่ายให้เหมาะสมกับโครงสร้างและความต้องการขององค์กรได้

Planning and implementing templates

เมื่อเริ่มต้นตั้งค่า SD-WAN environment ระบบจะมีเพียง **default templates** เท่านั้น โดยยังไม่มีการกำหนด VPNs แบบกำหนดเอง ในสภาวะเริ่มต้นนี้ อุปกรณ์ SD-WAN ทั้งหมดจะมีอินเทอร์เฟซอยู่ใน VPN 0 (transport VPN) ซึ่งช่วยให้อุปกรณ์สามารถสื่อสารกันในรูปแบบ full-mesh topology ได้ แต่หากต้องการให้สามารถส่งข้อมูลของผู้ใช้งาน SD-WAN fabric จำเป็นต้องกำหนด **Service VPN** ซึ่งหมายถึง VPN ใด ๆ ที่ไม่ใช่ VPN 0 หรือ VPN 512

การตั้งค่า VPN และอุปกรณ์ SD-WAN ดำเนินการผ่าน feature templates ซึ่งเป็นองค์ประกอบพื้นฐานในการกำหนดค่าต่าง ๆ ของอุปกรณ์ โดย feature templates จะถูกนำมารวมกันเป็น **device templates** และเชื่อมโยงกับอุปกรณ์ แต่ละตัว วิธีนี้เป็นแนวทางที่แนะนำในการกำหนดค่าอุปกรณ์ edge แทนการใช้ CLI แบบดั้งเดิม แม้ว่าจะสามารถสร้าง CLI templates ที่รองรับตัวแปรได้ แต่แนวทางนี้ถือว่าเป็นแบบเก่า และผู้ดูแลระบบควรให้ความสำคัญกับการใช้ feature templates เป็นหลัก

เนื่องจาก templates ส่วนใหญ่จะมีตัวแปร (variables) ที่ต้องกำหนดค่า เมื่อเชื่อมโยงกับอุปกรณ์ การวางแผนที่รอบคอบจะช่วยให้การนำไปใช้งานมีประสิทธิภาพมากขึ้น หากมีมาตรฐานที่ชัดเจนและลดข้อยุ่งเหยิงในการกำหนดค่าจะช่วยลดภาระในการจัดการในอนาคต การมีข้อยกเว้นมากเกินไปจะทำให้เกิด **template sprawl** หรือการกระจายตัวของเทมเพลตมากเกินไป ซึ่งทำให้ระบบซับซ้อนและยุ่งยากต่อการบริหารจัดการ

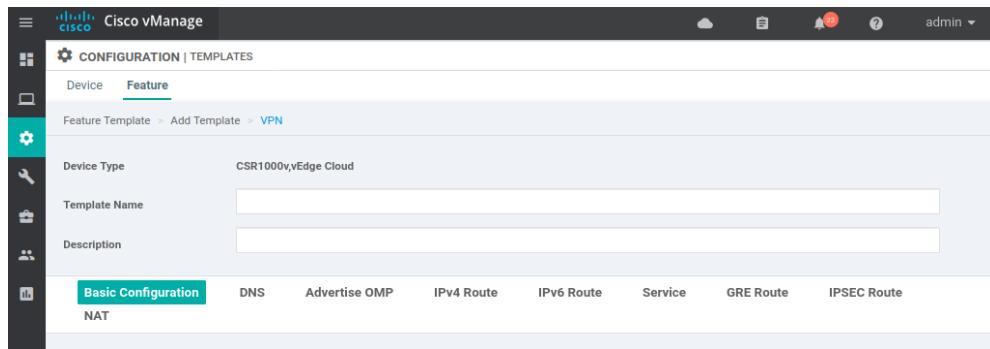
VPN 0 templates

อุปกรณ์ SD-WAN ถูกตั้งค่าเริ่มต้นด้วย manual ‘skinny’ (หรือ bootstrap) configurations เพื่อให้สามารถสื่อสารกันได้ในเบื้องต้น ซึ่งหมายความว่า VPN 0 ถูกกำหนดค่าแบบแม่นนวลด้วยตัวแปรที่ชัดเจนและลดข้อยุ่งเหยิงในการกำหนดค่าผ่าน templates สิ่งแรกที่ต้องทำคือสร้าง feature template สำหรับ VPN 0 เพื่อให้แน่ใจว่าการเชื่อมต่อระหว่างอุปกรณ์ SD-WAN จะไม่สูญหายเมื่อเริ่มใช้เทมเพลตสำหรับการตั้งค่าอื่น ๆ

ในขั้นตอนนี้ จะมีการเปลี่ยนแปลงค่าต่าง ๆ ให้น้อยที่สุด โดยคงค่าเริ่มต้นไว้มากที่สุดเพื่อสร้างพื้นฐานสำหรับการตั้งค่าขั้นสูงในอนาคต เป้าหมายหลักคือการเริ่มต้นส่งข้อมูลของผู้ใช้งาน SD-WAN fabric โดยใช้การกำหนดค่าที่เรียบง่ายที่สุด

เมื่อสร้างเทมเพลตและเลือกอุปกรณ์หลายตัว รายการของ sub-templates ที่สามารถใช้ได้จะถูกจำกัดให้แสดงเฉพาะเทมเพลตที่รองรับบนอุปกรณ์ทุกตัวที่เลือก ตัวอย่างเช่น หากเลือก CSR1000v และ vEdge Cloud พร้อมกัน ระบบจะแสดงเฉพาะ feature templates ที่สามารถใช้ได้กับทั้งสองอุปกรณ์ รวมถึงเทมเพลตเฉพาะของแต่ละอุปกรณ์ที่สามารถใช้ได้แยกกัน การทำความเข้าใจความแตกต่างนี้จะช่วยให้สามารถออกแบบเทมเพลตให้ครอบคลุมอุปกรณ์ได้อย่างมีประสิทธิภาพมากขึ้น

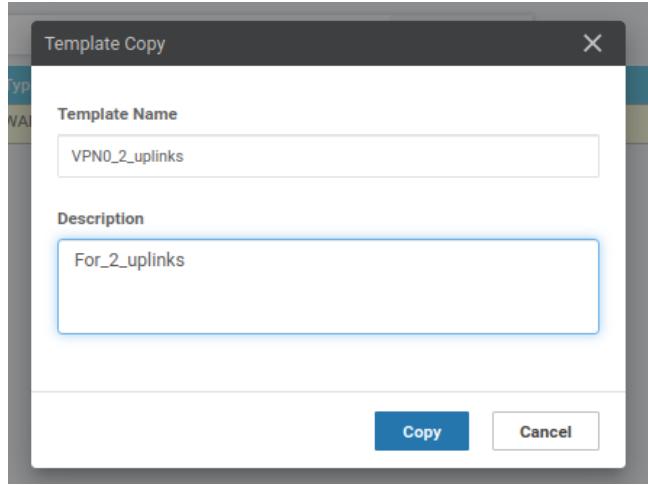
ใน vManage ให้ไปที่ [Configuration > Templates > Feature > Add Template](#) จากนั้นเลือก CSR1000v และ vEdge Cloud และคลิกที่ **VPN template** เพิ่มชื่อและคำอธิบายให้กับ template



นี่เป็นอีกส่วนหนึ่งที่ต้องใช้การพิจารณาและวางแผนอย่างรอบคอบในสภาพแวดล้อมการผลิต เทมเพลตที่ตั้งขึ้นดีจะทำให้การอ้างอิง เข้าใจ และจัดการได้ง่ายขึ้น นี่คือสิ่งที่คุณจะเก่งขึ้นเมื่อมีประสบการณ์ สำหรับการทดลองนี้ เราจะสร้างเทมเพลตสองอันสำหรับ VPNO โดยเทมเพลตหนึ่งจะถูกเชื่อมต่อกับอุปกรณ์ที่มี uplink เดียว และอีกเทมเพลตหนึ่งสำหรับอุปกรณ์ที่มีสอง uplinks ตั้งขึ้นเทมเพลตแรกว่า VPNO_1_uplink หลังจากตั้งขึ้นเทมเพลตและเพิ่มคำอธิบายแล้ว สิ่งสุดท้ายที่ต้องทำคือกำหนด static default route สำหรับ lab นี้ ให้คลิกที่ปุ่ม New IPv4 Route จากนั้นตั้งค่า Prefix เป็นค่า global 0.0.0.0/0 และคลิก Add Next Hop และกำหนดที่อยู่เป็นตัวแปร Device Specific โดยต้องตั้งชื่อตัวแปรให้มีชื่อกัน ในที่นี้เลือกใช้ชื่อ default_next_hop ค่าของตัวแปรนี้จะถูกกำหนดเมื่อนำเทมเพลตไปผูกกับอุปกรณ์ คลิก Add เพื่อบันทึกค่า next hop จากนั้นคลิก Add อีกครั้งเพื่อเพิ่ม default route ลงในเทมเพลต และสุดท้ายคลิก Save

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
VPNO_1_uplink	For_1_uplink	WAN Edge	CSR1000vEdge Cloud	0	0	admin	24 Feb 2025 5:58:...

เมื่อใช้เทมเพลต เราจะเห็นถึงประโยชน์ของการจัดการที่เป็นระบบ จากหน้าจอ feature templates ให้คลิกที่ สามจุดทางขวาของเทมเพลต VPNO_1_uplink และเลือก Copy ระบบจะแสดงกล่องโต๊ะอปให้แก้ไขชื่อและคำอธิบายของเทมเพลตใหม่ ซึ่งในกรณีสามารถตั้งชื่อเป็น VPNO_2_uplinks ได้



จากนั้นคลิกที่ สามจุด ทางขวาของแท็บของเทมเพลตใหม่ และเลือก [Edit](#) เพื่อดำเนินการแก้ไขเพิ่มเติม
สำหรับเทมเพลต [VPN0_2_uplinks](#) สิ่งเดียวที่ต้องเปลี่ยนคือการเพิ่ม next-hop ตัวที่สอง สำหรับ default route ของอุปกรณ์ที่มี dual uplinks ในแต่ละ VPN template สามารถกำหนดค่าเส้นทางเดียวกันได้เพียงครั้งเดียว แต่สามารถมีหลายเส้นทางในเทมเพลตเดียวกัน ใน Cisco IOS CLI แบบดั้งเดิม เราจะสร้าง static default routes สองรายการโดยใช้ next-hop ที่แตกต่างกัน แต่ใน VPN template เรากำหนดเพียง static default route เดียว และระบุ next-hops สองค่า แทน

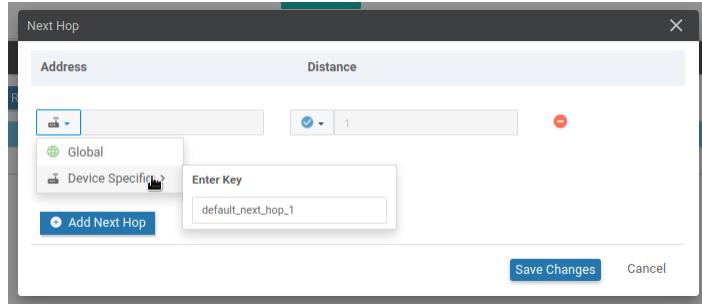
ให้คลิกไอคอน [pencil \(ดินสอ\)](#) ใต้ Action ของ default route

IPv4 ROUTE				
New IPv4 Route				
Optional	Prefix	Gateway	Selected Gateway Configuration	Action
<input type="checkbox"/>	0.0.0.0/0	Next Hop	1	

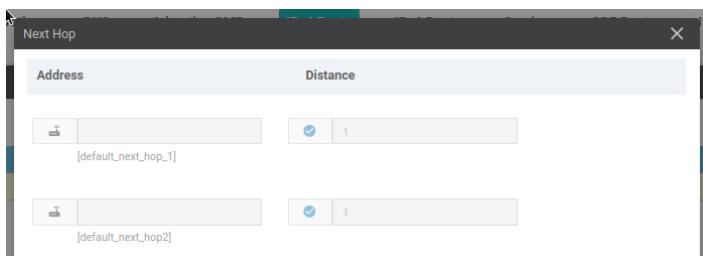
จากนั้นคลิกที่ [1 Next Hop](#) เพื่อแก้ไขค่าของ next-hop

Update IPv4 Route	
Prefix	0.0.0.0/0
Gateway	<input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN
Next Hop	1 Next Hop

เนื่องจากข้อตัวแปรต้องไม่ซ้ำกัน ให้เปลี่ยนชื่อ next-hop ปัจจุบัน เป็นชื่อใหม่ที่สามารถจำและอ้างอิงได้ง่ายเมื่อนำเทมเพลตไปใช้กับอุปกรณ์ ในที่นี้เลือกใช้ชื่อ [default_next_hop_1](#)



จากนั้นคลิก [Add Next Hop](#) และกำหนดตัวแปรใหม่สำหรับ next-hop ตัวที่สอง โดยตั้งชื่อเป็น [default_next_hop_2](#)



หลังจากกำหนดค่าเสร็จแล้ว คลิก [Save Changes](#) สองครั้ง และสุดท้ายคลิก [Update](#) เพื่อบันทึกการเปลี่ยนแปลงทั้งหมด

VPN Interface templates

VPN templates จะกำหนด VPN เอง แต่รายละเอียดต้องการ interface เพื่อต่อเข้าม VPN Interface templates จะอธิบาย การกำหนดค่าของ physical หรือ logical interfaces ซึ่งเป็นอีกพื้นที่หนึ่งที่ต้องมีการวางแผนและพิจารณาให้เหมาะสมกับสภาพแวดล้อม เทมเพลตส่วนใหญ่ควรครอบคลุมตัวเลือกที่กว้างที่สุดและเป็นมาตรฐาน (เช่น ตัวเลือกที่ใช้งานมากที่สุด)

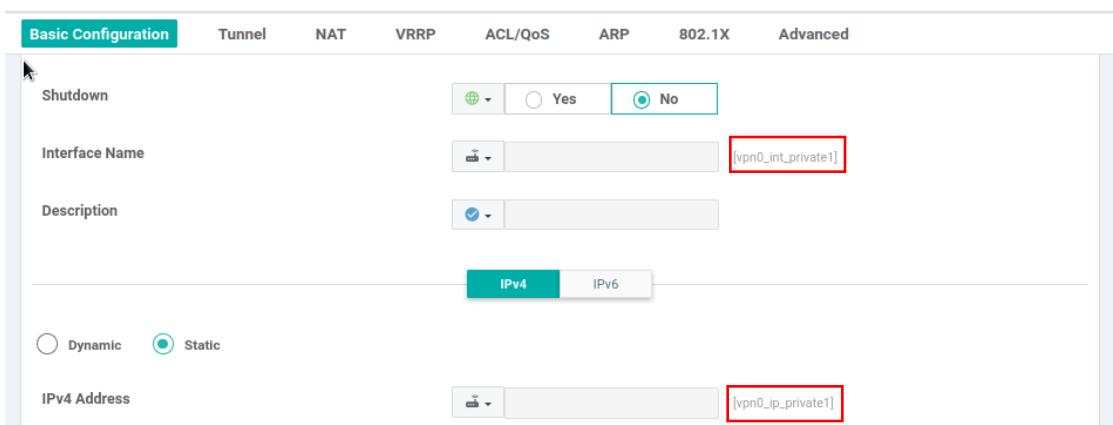
จะมีการแยกเปลี่ยนระหว่างจำนวนเทมเพลตและปริมาณข้อมูลที่ต้องป้อนผ่านตัวแปร เพื่อช่วยในการตัดสินใจนี้ ควรพิจารณาสิ่งที่เป็นไปได้ทั่วไปและสิ่งที่แตกต่างกันในสิ่งที่คุณพยายามทำ ใน topology นี้ ลิงก์ทั้งหมดเป็น full-duplex gigabit Ethernet ที่ใช้ static IP addressing ซึ่งมีลักษณะร่วมกัน ความแตกต่างจะอยู่ที่ชื่อของอินเทอร์เฟซ ว่าจะสามารถรองรับ 802.1Q-tagged traffic หรือไม่ และจะอยู่ใน transport VPN หรือ service VPN

เมื่อเทมเพลตอินเทอร์เฟซถูกกำหนดให้กับ device template แล้ว จะสามารถใช้งานได้เพียงครั้งเดียวต่อ VPN นั้น หมายความว่า **สำหรับอุปกรณ์ที่มี dual uplinks จะต้องสร้าง interface templates แยกกันสองชุด** เพื่อให้ลดจำนวนเทมเพลต ควรกำหนดสิ่งที่เป็นทั่วไปในจำนวนมากที่สุดของไซต์ของเรา ตัวอย่างเช่น หากไซต์สาขาส่วนใหญ่ถูกตั้งค่าให้ WAN interface แรก เชื่อมต่อกับ MPLS L3VPN ในขณะที่ WAN interface ที่สอง เชื่อมต่อกับ public Internet service เราสามารถสร้างเทมเพลตสำหรับแต่ละประเภทการขนส่ง ซึ่งเป็นสิ่งที่เราจัดทำใน lab นี้

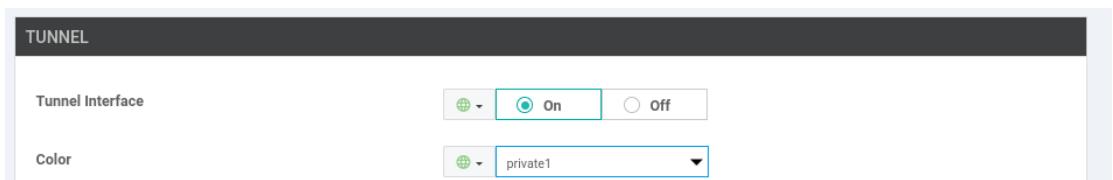
เริ่มต้นโดยการสร้าง [feature template](#) ใหม่ และเลือกประภากับอุปกรณ์ [CSR1000v](#) และ [vEdge Cloud](#) จากนั้นคลิกที่ [VPN Interface Ethernet template type](#) ตั้งชื่อเทมเพลตนี้ว่า [VPN0_private1](#)



ตั้งค่า Shutdown เป็นค่า global no และตั้งชื่อ Interface Name เป็นตัวแปรเฉพาะอุปกรณ์ vpn0_int_private1 นอกจานี้ยังต้องตั้งค่า IPv4 Address เป็นตัวแปรเฉพาะอุปกรณ์ vpn0_ip_private1



ให้ตั้งค่า Tunnel Interface เป็นค่า global on และ Color เป็นค่า global private1 แล้วคลิก Save ที่ด้านล่างเพื่อทำการบันทึกเมมเพลต



จากนั้น ในส่วนของ Feature Template ให้คัดลอกเทมเพลตก่อนหน้านี้ และตั้งชื่อใหม่ว่า VPN0_public-internet



ทำการแก้ไขตัวแปรทั้งหมดเพื่อเปลี่ยนจาก private1 เป็น public-internet

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	
VPNO_...	VPNO_private1	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 6:20...	...
VPNO_...	For_1_uplink	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 5:58...	...
VPNO_...	VPNO_public-internet	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 6:23...	...
VPNO_...	For_2_uplinks	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 6:07...	...

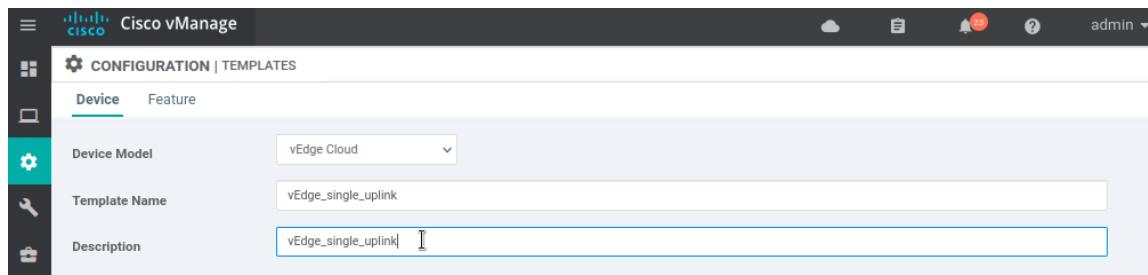
Device templates

เพื่อให้เข้าใจแนวทางการทำงานและเริ่มเห็น templates ใน การใช้งาน จะสร้างและนำ device templates ไปใช้สำหรับ SD-WAN edges สามชุดที่เรามีอยู่ **Device templates** คือชุดรวมของ **feature templates** นอกจากนี้ยังสามารถสร้าง device templates โดยใช้ CLI ซึ่งอาจเป็นประโยชน์สำหรับการเปลี่ยนไปใช้ SD-WAN จากทักษะในอดีต แต่ถือว่าเป็นวิธีการที่ไม่นิยมใน Lab นี้

การสร้าง device templates จะทำเป็นรายประเภทอุปกรณ์ เพื่อให้สามารถกำหนดค่าไฟล์เจอร์ที่เกี่ยวข้องกับอุปกรณ์นั้นได้ แต่สามารถมีเทมเพลตหลายชุดสำหรับอุปกรณ์ชนิดเดียวกัน ใน lab นี้เราจะสร้าง device templates สองชุด หนึ่งชุดสำหรับ vEdge และอีกหนึ่งชุดสำหรับ cEdges

สำหรับ lab topology นี้ เราต้องการเพียงสอง device templates เพราะ cEdge sites ทั้งสองแห่งมี dual uplinks หากใช้ตัวนี้มี single uplink ขณะที่อีกตัวมี dual uplinks เราจะต้องสร้าง device templates แยกกันเพื่อรับความแตกต่างนี้ เมื่อว่าจะเป็นอุปกรณ์ประเภทเดียวกัน นี้เป็นอีกจุดที่การวางแผนและการมาตรฐานเมื่อต้องนำ Cisco SD-WAN ไปใช้งาน

จากเมนู Configuration > Templates > Device ให้คลิกที่ปุ่ม Create Template และเลือก From Feature Template จากนั้นเลือก vEdge Cloud เป็นโมเดล/oุปกรณ์ ตั้งชื่อเทมเพลตนี้ว่า vEdge_single_uplink



สำหรับตอนนี้ การตั้งค่าเพียงอย่างเดียวที่เราต้องเปลี่ยนคือการเปลี่ยน VPN 0 template เป็น VPNO_1_uplink และ VPN Interface ที่เกี่ยวข้องเป็น VPNO_private1



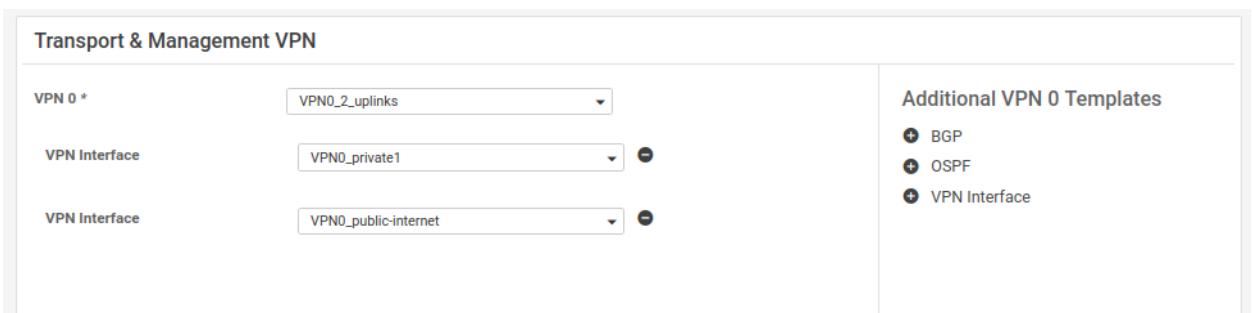
แม้ว่าเราจะไม่ใช้ VPN 512 interface ในขณะนี้ แต่ยังคงต้องระบุในโหมดเพลต สำหรับ vEdge ดังนั้นให้เลือก **factory default, VPN interface** และเพิ่ม **default template** จากนั้นคลิกปุ่ม **Create** ที่ด้านล่าง



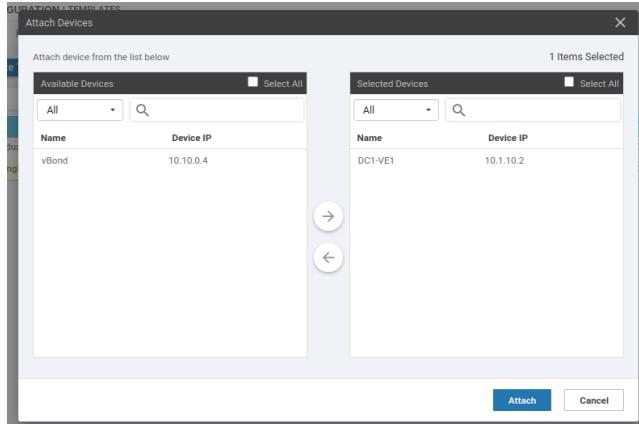
สร้าง device template อีกชุดหนึ่ง และเลือก CSR1000v โดยตั้งชื่อว่า **CSR1Kv_dual_uplink** ในเวอร์ชันของ vManage code นี้ cEdge templates จะระบุ AAA และ Cisco-AAA templates ซึ่งไม่สามารถใช้ร่วมกันได้ ให้เปลี่ยน **AAA template** เป็น **None** ตั้งค่า **VPN 0** เป็น **VPN0_2_uplinks** และ **VPN Interface** เป็น **VPN0_private1**



ในส่วน **Additional VPN 0 Templates** ให้เพิ่ม **VPN Interface** ใหม่และตั้งค่าเป็น **VPN0_public-internet** จากนั้นคลิกปุ่ม **Create** ที่ด้านล่าง

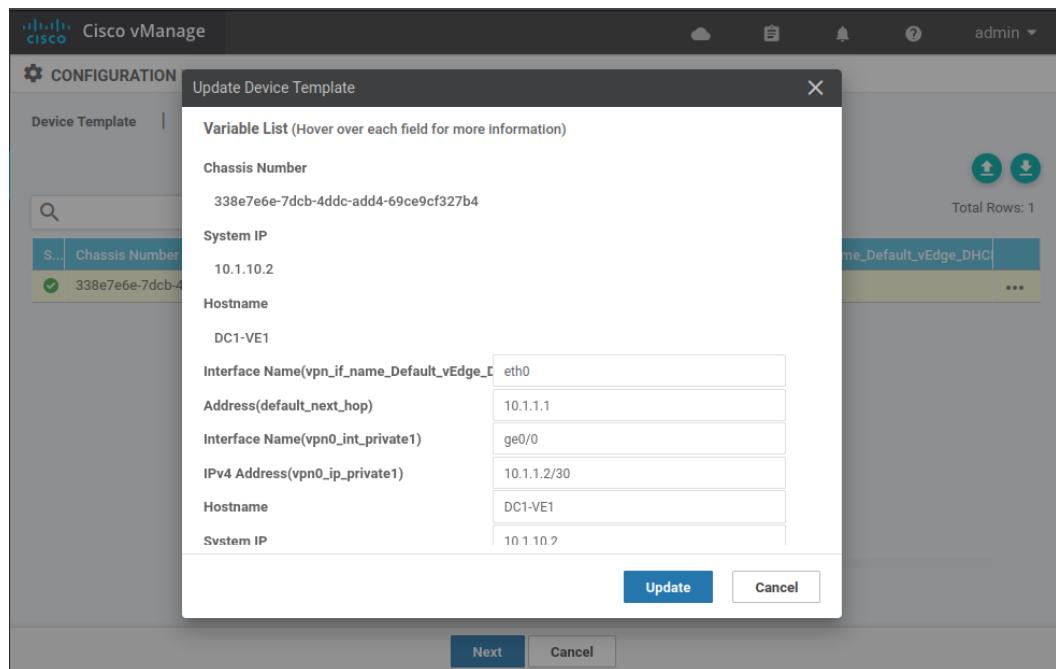


ตอนนี้เราจะนำโหมดเพลตไปใช้กับอุปกรณ์ ให้คลิกที่สามจุดด้านขวาของแล้ว **vEdge_single_uplink** และเลือก **Attach Devices** จากนั้นเลือก **DC1-VE1** จากรายการแล้วคลิก **Attach**



ในขั้นตอนนี้ เราเมต้าเลือกในการกำหนดค่าตัวแปรแต่ละตัวโดยตรง หรือการนำเข้าและส่งออกไฟล์ CSV หากเรามีอุปกรณ์มากกว่าห้าชุด การกำหนดค่าอุปกรณ์โดยใช้ไฟล์ CSV จะรวดเร็วมาก

คลิกที่สามจุดแล้วเลือก [Edit Device Template](#) ตอนนี้ เราจะเห็นตัวแปรที่เราสร้างขึ้นภายใน [feature templates](#) เราควรจะสามารถเห็นได้ทันทีว่าการตั้งค่าตัวแปรที่ดีแล้วมีความหมายมีความสำคัญมาก ตัวแปรและค่าของ [DC1-VE1](#) ได้แก่:



คลิก [Update](#) แล้วคลิก [Next](#)

ตอนนี้เราจะเห็นหน้าจอ 'pre-provisioning' ไม่ต้องทำอะไรที่นี่ และสามารถคลิก [Configure Devices](#) เพื่อดำเนินการต่อหากต้องการ อย่างไรก็ตาม เราสามารถคลิกที่อุปกรณ์ใดก็ได้ในรายการเพื่อดูว่าการกำหนดค่าที่จะนำไปใช้เป็นอย่างไร เปรียบเทียบกับการกำหนดค่าปัจจุบัน และตั้งค่าตัวจับเวลาการย้อนกลับในกรณีที่การกำหนดค่าใหม่ทำให้การสื่อสารกับ controller ล้มเหลว โดยเฉพาะไฟล์ config diff นั้นจะมีประโยชน์มาก หลังจากที่เราคลิก [Configure Devices](#) การกำหนดค่าจะ

ถูกส่งไปยังอุปกรณ์ต่างๆ เราสามารถดูความก้าวหน้า และหากเกิดข้อผิดพลาด การกำหนดค่าจะถูกยก้อนกลับและคุณควรได้รับข้อมูลเกี่ยวกับสาเหตุที่การกำหนดค่าล้มเหลว

The screenshot shows the Cisco vManage interface under the 'TASK VIEW' tab. A specific task titled 'Push Feature Template Configuration' has been completed successfully ('Validation Success'). The task details indicate it was initiated by 'admin' from IP '10.0.0.10'. The table below lists the task results, showing one entry where the status is 'Success' and the message is 'Done - Push F...'. The table includes columns for Status, Message, Chassis Number, Device Model, Hostname, System IP, Site ID, and vManage IP.

	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
>	Success	Done - Push F...	338e7e6e-7dc8-4dd...	vEdge Cloud	DC1-VE1	10.1.10.2	10000	10.0.0.101

กลับไปที่ส่วน device templates และแนบ cEdges สองตัวเข้ากับ CSR1Kv template นี้คือค่าที่ผู้สอนใช้สำหรับ lab นี้:

S100-CE1:

System IP	10.100.10.2
Hostname	S100-CE1
Address(default_next_hop_1)	198.51.100.5
Address(default_next_hop_2)	203.0.113.5
Interface Name(vpn0_int_public-internet)	GigabitEthernet2
IPv4 Address(vpn0_ip_public-internet)	203.0.113.6/30
Interface Name(vpn0_int_private1)	GigabitEthernet1
IPv4 Address(vpn0_ip_private1)	198.51.100.6/30
Hostname	S100-CE1
System IP	10.100.10.2
Site ID	100

S200-CE1:

System IP	10.200.10.2
Hostname	S200-CE1
Address(default_next_hop_1)	198.51.100.9
Address(default_next_hop_2)	203.0.113.9
Interface Name(vpn0_int_public-internet)	GigabitEthernet2
IPv4 Address(vpn0_ip_public-internet)	203.0.113.10/30
Interface Name(vpn0_int_private1)	GigabitEthernet1
IPv4 Address(vpn0_ip_private1)	198.51.100.10/30
Hostname	S200-CE1
System IP	10.200.10.2
Site ID	200

เมื่อค่าทั้งหมดถูกป้อนและการกำหนดค่าได้ถูกนำไปใช้ หวังว่าทุกอย่างจะเป็นไปด้วยดีและอุปกรณ์ทั้งหมดของเรายังออนไลน์อยู่ ณ จุดนี้ ตอนนี้เราพร้อมที่จะเริ่มนำข้อมูลผู้ใช้เข้าสู่ SD-WAN แล้ว

	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
>	Success	Done - Push F...	CSR-e6bcd73a-88a2...	CSR1000v	S100-CE1	10.100.10.2	100	10.0.0.101
>	Success	Done - Push F...	CSR-ea80abbc-13cf...	CSR1000v	S200-CE1	10.200.10.2	200	10.0.0.101

Service VPN

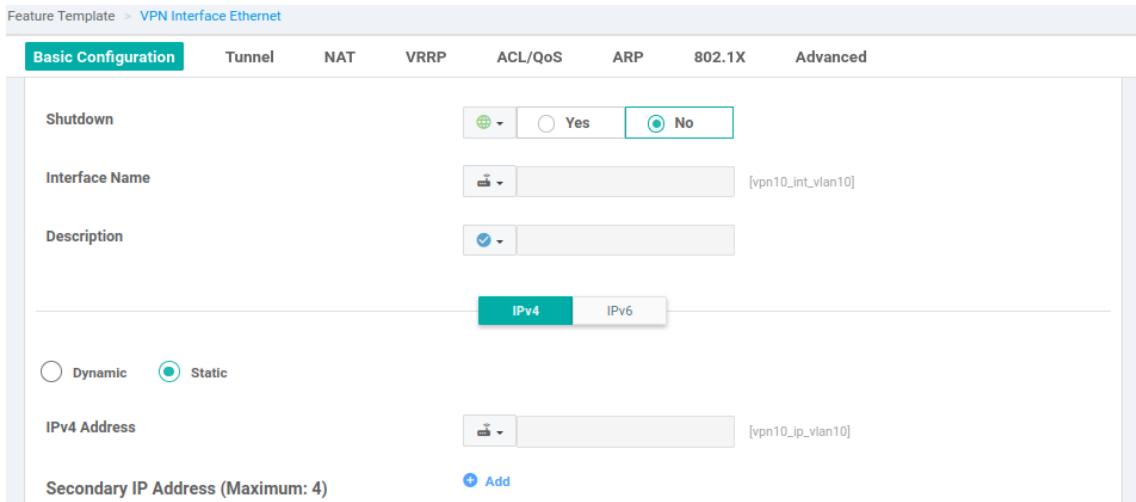
อย่างที่เราได้เห็นแล้ว จะใช้เวลาค่อนข้างมากในการเตรียมความพร้อมก่อนที่คุณจะเริ่มส่งข้อมูลผู้ใช้ผ่าน SD-WAN ได้ โชคดีที่กระบวนการพื้นฐานในการเพิ่ม Service VPN นั้นมีความคล้ายคลึงกับสิ่งที่เราได้กล่าวถึงไปแล้ว Service VPNs ใช้ในการส่งข้อมูลผู้ใช้ และเป็น VPN โดยที่มี ID แตกต่างจาก 0 หรือ 512 ตั้งแต่เวอร์ชัน v19.2 เป็นต้นไป เราสามารถมี VPN ทั้งหมด 64 รายการใน fabric เดียว

จากส่วน configuration template ใน vManage ให้สร้าง feature template ใหม่และเลือกอุปกรณ์ CSR1000V และ vEdge Cloud จากนั้นเลือก VPN template สำหรับ template นี้ ตั้งชื่อว่า **VPN10_basic** ตั้งค่า **VPN global 10** ในส่วน Advertise OMP ให้ตั้งค่า **Static** และ **Connected** เป็น **global on** แล้วคลิกที่ปุ่ม **Save** ที่ด้านล่าง

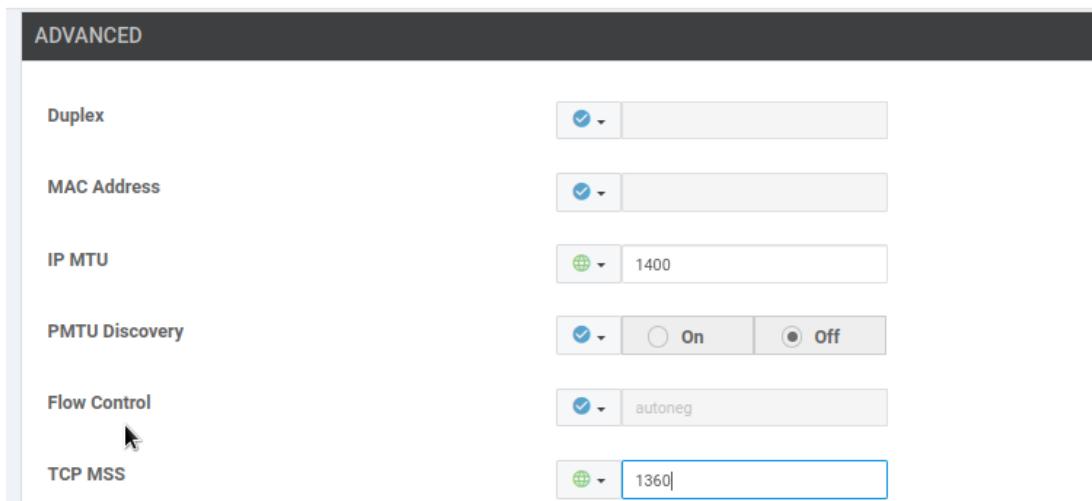
Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
VPN0....	VPN0_public-internet	WAN E...	CSR1000v vEdge Cloud	1	2	admin	24 Feb 2025 6:23:...
VPN0....	For_2_uplinks	WAN E...	CSR1000v vEdge Cloud	1	2	admin	24 Feb 2025 6:07:...
VPN0....	For_1_uplink	WAN E...	CSR1000v vEdge Cloud	1	1	admin	24 Feb 2025 5:58:...
VPN0....	VPN0_private1	WAN E...	CSR1000v vEdge Cloud	2	3	admin	24 Feb 2025 6:20:...
VPN10...	VPN10_basic	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 8:32:...

ถัดไป เราต้องสร้าง VPN interface templates สำหรับ Service VPN นี้ อีกครั้ง เราต้องพิจารณาว่าสำหรับแต่ละอุปกรณ์ เราสามารถใช้ VPN interface template ได้เพียงครั้งเดียวต่อ VPN ดังนั้นหากเรามีหลาย interface ที่เข้าร่วมใน VPN เดียวกันบนอุปกรณ์เดียว เราต้องใช้ interface template ที่แตกต่างกันสำหรับแต่ละ interface สำหรับ lab นี้ อุปกรณ์ SD-WAN ทั้งหมดของเรามี LAN-facing subinterfaces สามตัว ดังนั้นเราจะต้องการ VPN interface templates สามตัว

ให้สร้าง feature template ใหม่ โดยเลือกอุปกรณ์ CSR1000V และเลือก VPN Interface Ethernet template ตั้งชื่อว่า VPN10_int_vlan10 ตั้งค่าค่า Shutdown เป็น global no และตั้งชื่อ interface เป็นตัวแปรเฉพาะของอุปกรณ์ vpn10_int_vlan10 เราจะใช้ที่อยู่ IP แบบ static ดังนั้น ให้ตั้งค่าที่อยู่ IPv4 เป็นตัวแปรเฉพาะของอุปกรณ์ vpn10_ip_vlan10



การตั้งค่าครั้งสุดท้ายที่เราจะเปลี่ยนแปลงสำหรับ template นี้ในขณะนี้คือภายใต้ส่วน Advanced เราต้องเปลี่ยนค่า IP MTU เป็น global 1400 และ TCP MSS เป็น global 1360 นี่คือค่าที่เป็น ‘catch-all’ และก็ใช้ได้สำหรับ lab แต่เป็นสิ่งที่ต้องพิจารณาอย่างจริงจังในเครือข่าย Production ด้วย DMVPN tunnels การตั้งค่าเหล่านี้เป็นสิ่งที่พอดีทั่วไป มาตรฐาน MTU คือ 1500 และอุปกรณ์ edge จะต้องทำการแบ่งส่วน packet หาก MTU ถูกตั้งค่าต่ำกว่าและอุปกรณ์ที่เชื่อมต่อกับ subnet ไม่ได้รับการปรับเปลี่ยนให้สอดคล้อง



ในทางปฏิบัติ สำหรับข้อมูลผู้ใช้ทั่วไป นี่อาจไม่ใช่ปัญหาใหญ่ โดยเฉพาะสำหรับสำนักงานสาขาขนาดเล็กที่มีปริมาณการจราจรต่ำ อีกสิ่งที่ต้องพิจารณาในออกแบบ Cisco SD-WAN คือ หากเราจะใช้ 802.1Q-tagged subinterfaces (ซึ่งเราจะใช้ใน

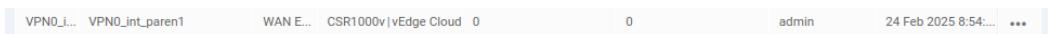
lab นี้) เมื่อตั้งค่า subinterfaces ที่ติดแท็ก เราจะต้องตั้งค่า parent interface ให้มี MTU ที่สูงกว่าอย่างน้อย 4 ไบต์ (เช่น 1504) หรือกำหนดให้ subinterfaces ทั้งหมดมี MTU ต่ำกว่าที่ตั้งไว้ 4 ไบต์ เมื่อเราตั้งค่า MTU เป็น 1400 และตรวจสอบว่าอุปกรณ์ที่เชื่อมต่อของเรายังได้รับการกำหนดค่าให้สอดคล้อง เราจะสามารถรองรับความต้องการเพิ่มเติมจากการ encapsulations ต่างๆ (802.1Q, IPsec, ฯลฯ) ได้

ให้คัดลอก Template อีกสองครั้งและเปลี่ยนค่าของ VLAN เป็น 20 และ 30 ตามลำดับ

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	Actions
VPN10...	VPN10_int_vlan20	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 8:47:...	...
VPN10...	VPN10_int_vlan30	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 8:48:...	...
VPN10...	VPN10_int_vlan10	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 8:44:...	...
VPN0...	VPN0_public-internet	WAN E...	CSR1000v vEdge Cloud	1	2	admin	24 Feb 2025 6:23:...	...
VPN0...	For_2_uplinks	WAN E...	CSR1000v vEdge Cloud	1	2	admin	24 Feb 2025 6:07:...	...
VPNO...	For_1_uplink	WAN E...	CSR1000v vEdge Cloud	1	1	admin	24 Feb 2025 5:58:...	...
VPNO...	VPNO_private1	WAN E...	CSR1000v vEdge Cloud	2	3	admin	24 Feb 2025 6:20:...	...
VPN10...	VPN10_basic	WAN E...	CSR1000v vEdge Cloud	0	0	admin	24 Feb 2025 8:32:...	...

เมื่อใช้ subinterfaces, parent interface จะต้องมี template ของตัวเองด้วย และมันจะต้องอยู่ใน VPN 0 หากเรามี subinterfaces โดยไม่มี parent interface ที่อยู่ใน VPN 0 เราจะได้รับข้อผิดพลาดเมื่อพยายามส่ง template ออกไป ถึงแม้ว่า parent interface จะอยู่ใน VPN 0 แต่ มันจะไม่ทำการเชื่อมต่อ tunnels และจะไม่มีการกำหนด IP address ซึ่งจะทำหน้าที่เป็น placeholder

สามารถคัดลอกหนึ่งใน template ก่อนหน้านี้และเปลี่ยนชื่อเป็น [VPNO_int_parent1](#) เปลี่ยนชื่อ Interface เป็น [vpn0_int_parent1](#) และตั้งค่าที่อยู่ [IPv4](#) เป็นค่า [default](#) นอกจากนี้ให้ตั้งค่า IP MTU และ TCP MSS เป็นค่า [default](#) ด้วย



ตอนนี้สามารถแนบ template ไปยังอุปกรณ์ได้ จากส่วนการ configuration [device templates](#) ให้แก้ไข template ของ vEdge ภายใต้ [VPN 0](#) เพิ่ม [VPN Interface](#) ใหม่และอ้างอิงถึง template [VPNO_int_parent1](#)

จากนั้นคลิกที่เครื่องหมายบวกด้านหลัง [Service VPN](#) และเลือก [VPNO_basic](#) จาก dropdown คลิก [VPN Interface](#) สามครั้งและเลือกสาม [VLAN interface](#) templates จากนั้นคลิกที่ปุ่ม Update เพื่อบันทึกการเปลี่ยนแปลงของ device template

The screenshot shows the 'Service VPN' configuration page. It has tabs for 'Basic Information', 'Transport & Management VPN', 'Service VPN' (which is selected), and 'Additional Templates'. Under 'Service VPN', there are three sections for 'VPN Interface' assigned to 'VPN10_int_vlan10', 'VPN10_int_vlan20', and 'VPN10_int_vlan30'. To the right, a sidebar titled 'Additional VPN Templates' lists various protocols and interfaces.

เราจะเห็นรายการอุปกรณ์ที่ต้องกรอกค่าตัวแปร คลิกที่สามจุดทางด้านขวาของอุปกรณ์และเลือก [Edit Device Template](#) ค่าที่ใช้สำหรับ lab นี้มีดังนี้:

Interface Name(vpn_if_name_Default_vEdge_DHCP_Tunnel)	eth0
Address(default_next_hop)	10.1.1.1
Interface Name(vpn0_int_private1)	ge0/0
IPv4 Address(vpn0_ip_private1)	10.1.1.2/30
Hostname	DC1-VE1
System IP	10.1.10.2
Site ID	10000
Interface Name(vpn10_int_vlan30)	ge0/1.30
IPv4 Address(vpn10_ip_vlan30)	10.1.30.1/24
Interface Name(vpn10_int_vlan20)	ge0/1.20
IPv4 Address(vpn10_ip_vlan20)	10.1.20.1/24
Interface Name(vpn10_int_vlan10)	ge0/1.10
IPv4 Address(vpn10_ip_vlan10)	10.1.10.1/24
Interface Name(vpn0_int_parent1)	ge0/1

	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP	Total Row
✓	Success	Done - Push Feat...	338e7e6e-7dcb-4dd...	vEdge Cloud	DC1-VE1	10.1.10.2	10000	10.0.0.101	
[24-Feb-2025 14:34:35 UTC] Configuring device with feature template: vEdge_single_uplink [24-Feb-2025 14:34:35 UTC] Generating configuration from template [24-Feb-2025 14:34:37 UTC] Checking and creating device in vManage [24-Feb-2025 14:34:38 UTC] Device is online [24-Feb-2025 14:34:38 UTC] Updating device configuration in vManage [24-Feb-2025 14:34:39 UTC] Pushing configuration to device [24-Feb-2025 14:34:52 UTC] Template successfully attached to device									

ทำการขั้นตอนเดียวกันสำหรับเพลตอุปกรณ์ cEdge เพิ่มอินเทอร์เฟชหลัก VPN 0, VPN 10 service VPN และสามชั้บอินเทอร์เฟซ

S100-CE1:

Address(default_next_hop_1)	198.51.100.5
Address(default_next_hop_2)	203.0.113.5
Interface Name(vpn0_int_public-internet)	GigabitEthernet2
IPv4 Address(vpn0_ip_public-internet)	203.0.113.6/30
Interface Name(vpn0_int_private1)	GigabitEthernet1
IPv4 Address(vpn0_ip_private1)	198.51.100.6/30
Hostname	S100-CE1
System IP	10.100.10.2
Site ID	100
Interface Name(vpn10_int_vlan30)	GigabitEthernet3.30
IPv4 Address(vpn10_ip_vlan30)	10.100.30.1/24
Interface Name(vpn10_int_vlan20)	GigabitEthernet3.20
IPv4 Address(vpn10_ip_vlan20)	10.100.20.1/24
Interface Name(vpn10_int_vlan10)	GigabitEthernet3.10
IPv4 Address(vpn10_ip_vlan10)	10.100.10.1/24
Interface Name(vpn0_int_parent1)	GigabitEthernet3

S200-CE1:

Address(default_next_hop_1)	198.51.100.9
Address(default_next_hop_2)	203.0.113.9
Interface Name(vpn0_int_public-internet)	GigabitEthernet2
IPv4 Address(vpn0_ip_public-internet)	203.0.113.10/30
Interface Name(vpn0_int_private1)	GigabitEthernet1
IPv4 Address(vpn0_ip_private1)	198.51.100.10/30
Hostname	S200-CE1
System IP	10.200.10.2
Site ID	200
Interface Name(vpn10_int_vlan30)	GigabitEthernet3.30
IPv4 Address(vpn10_ip_vlan30)	10.200.30.1/24
Interface Name(vpn10_int_vlan20)	GigabitEthernet3.20
IPv4 Address(vpn10_ip_vlan20)	10.200.20.1/24
Interface Name(vpn10_int_vlan10)	GigabitEthernet3.10
IPv4 Address(vpn10_ip_vlan10)	10.200.10.1/24
Interface Name(vpn0_int_parent1)	GigabitEthernet3

Push Feature Template Configuration Validation Success									Initiated By: admin From: 10.0.0.10
Total Task: 2 Success : 2									Total Rows: 2
	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP	
>	Success	Done - Push Feat...	CSR-e6bcd73a-88a2...	CSR1000v	S100-CE1	10.100.10.2	100	10.0.0.101	
>	Success	Done - Push Feat...	CSR-ea80abbc-13cf...	CSR1000v	S200-CE1	10.200.10.2	200	10.0.0.101	

สำเร็จ!

ในขั้นตอนนี้ เราควรสามารถส่ง pings ไปยังที่อยู่ .1 หรือ .254 ได้ๆ จากทั้งเราเตอร์ edge และสวิตช์ที่เชื่อมต่ออยู่ภายใน VPN 10 ได้

```
Compressed configuration from 1159 bytes to 743 bytes[OK]
S200-SW1#ping 10.1.30.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.30.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4 ms
S200-SW1#ping 10.100.30.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.30.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
S200-SW1#
```

ในการที่ Ping ไม่ได้ ลองตรวจสอบการกำหนดค่าใน Templates อีกรอบ ว่าในส่วนของ Shutdown ได้เลือกเป็น No หรือไม่ เพราะเราอาจจะไม่ได้สั่งเปิด Port ผ่าน Template

```
CSR
S200-CE1(config-if)#
*S200-CE1(config-if)#
*Feb 24 14:56:55.393: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by vmanage-admin, transaction-id 870
*Feb 24 14:59:27.203: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by vmanage-admin, transaction-id 891
*Feb 24 15:01:05.782: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by vmanage-admin, transaction-id 976
S200-CE1(config-if)#
S200-CE1(config-if)#
Uncommitted changes found, commit them? [yes/no/CANCEL] no

S200-CE1#show ip int b
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1   198.51.100.10  YES other up        up
GigabitEthernet2   203.0.113.10  YES other up        up
GigabitEthernet3   unassigned     YES unset administratively down down
GigabitEthernet3.10 10.200.10.1   YES other administratively down down
GigabitEthernet3.20 10.200.20.1  YES other administratively down down
GigabitEthernet3.30 10.200.30.1  YES other administratively down down
GigabitEthernet4   unassigned     YES unset up        up
Loopback65528     192.168.1.1   YES other up        up
Tunnel1           198.51.100.10  YES TFTP up        up
Tunnel2           203.0.113.10  YES TFTP up        up
S200-CE1#
```

แก้ไขแล้ว Push ใหม่

```

Tunnell           198.51.100.10  YES TFTP   up          up
Tunnel2          203.0.113.10  YES TFTP   up          up
S200-CE1#[vmxnet3][WR][vmxnet3_get_command_status]: Received request for unknown
command: cafe000f

*Feb 24 15:03:21.388: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF
DNF by vmanage-admin, transaction-id 995
*Feb 24 15:03:27.864: %LINK-3-UPDOWN: Interface GigabitEthernet3, changed state
to up
*Feb 24 15:03:28.864: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3, changed state to up
S200-CE1#show ip int b
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1    198.51.100.10  YES other up          up
GigabitEthernet2    203.0.113.10  YES other up          up
GigabitEthernet3    unassigned     YES unset up          up
GigabitEthernet3.10 10.200.10.1   YES other up          up
GigabitEthernet3.20 10.200.20.1   YES other up          up
GigabitEthernet3.30 10.200.30.1   YES other up          up
GigabitEthernet4    unassigned     YES unset up          up
Loopback65528      192.168.1.1   YES other up          up
Tunnell            198.51.100.10  YES TFTP   up          up
Tunnel2            203.0.113.10  YES TFTP   up          up
S200-CE1#

```

```

S200-SW1#trace 10.1.10.254
Type escape sequence to abort.
Tracing the route to 10.1.10.254
VRF info: (vrf in name/id, vrf out name/id)
  1 10.200.10.1 2 msec 2 msec 2 msec
  2 10.1.10.1 3 msec 2 msec 3 msec
  3 *
      10.1.10.254 3 msec 3 msec
S200-SW1#

```

การใช้คำสั่ง traceroute จะแสดงให้เห็นว่า S200-CE1 เป็น hop แรก จากนั้นการขนส่งพื้นฐานจะมองไม่เห็นโดยสิ้นเชิง จนกว่าจะถึง DC1-VE1 (เมื่อถูกกับ MPLS L3VPN ที่ปิดการเผยแพร่ TTL) จริงๆ แล้วสิ่งนี้ลือกกว่าการใช้งาน L3VPN ของ SP แบบดั้งเดิม เพราะว่า edge จะอยู่หลังการกระโดยเดาหมายค้างภายในศูนย์ข้อมูลที่อยู่หลังไฟร์วอลล์ edge ที่เชื่อมต่อกับ SP

จาก cEdge เราสามารถดูตารางการกำหนดเส้นทาง VPN ได้ เช่นเดียวกับ VRF แบบดังเดิม:

```

S100-CE1>show ip route vrf 10
Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, m - OSPF
      n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      H - NHRP, G - NHRP registered, g - NHRP registration summary
      o - ODR, P - periodic downloaded static route, l - LIS
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set

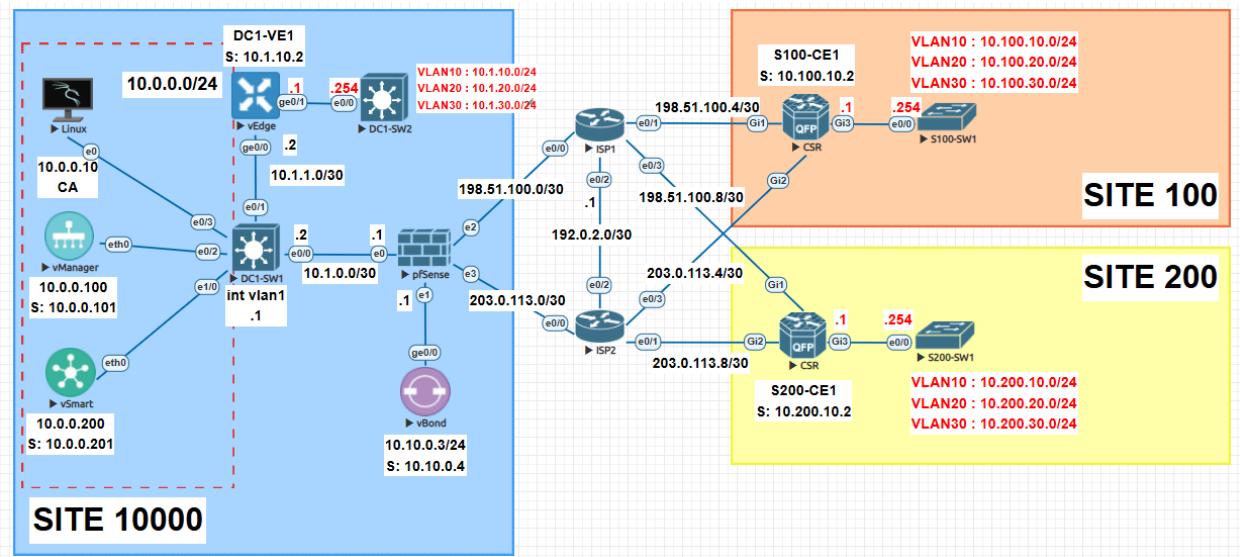
      10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
m        10.1.10.0/24 [251/0] via 10.1.10.2, 00:18:04
m        10.1.20.0/24 [251/0] via 10.1.10.2, 00:18:04
m        10.1.30.0/24 [251/0] via 10.1.10.2, 00:18:04
C        10.100.10.0/24 is directly connected, GigabitEthernet3.10
L        10.100.10.1/32 is directly connected, GigabitEthernet3.10
C        10.100.20.0/24 is directly connected, GigabitEthernet3.20
L        10.100.20.1/32 is directly connected, GigabitEthernet3.20
C        10.100.30.0/24 is directly connected, GigabitEthernet3.30
L        10.100.30.1/32 is directly connected, GigabitEthernet3.30
m        10.200.10.0/24 [251/0] via 10.200.10.2, 00:39:22
m        10.200.20.0/24 [251/0] via 10.200.10.2, 00:39:22
m        10.200.30.0/24 [251/0] via 10.200.10.2, 00:39:22
S100-CE1>

```

เราสามารถดูรายละเอียดเพิ่มเติมจากบรรทัดคำสั่งด้วยคำสั่งต่างๆ เช่น show sdwan omp แต่เน้นอนว่าในนี้เป็นวิธีการแบบเก่า เราสามารถเข้าถึงข้อมูลเดิมๆ กัน (และข้อมูลเพิ่มเติมอีกมาก) ผ่าน vManage โดยไปที่ [Monitor > Network > Device > Real Time](#) และเลือกข้อมูลที่ต้องการ เช่น [OMP Received Routes](#)

The screenshot displays two main sections of the Cisco vManage interface:

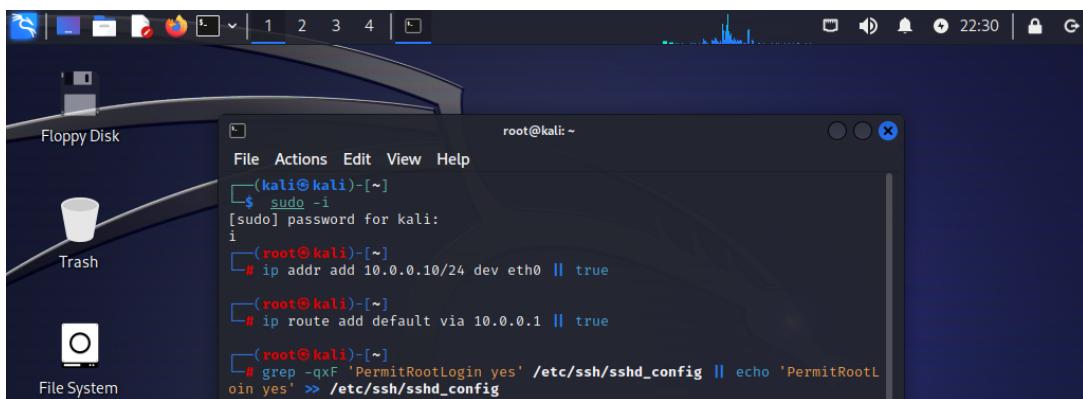
- OMP Received Routes:** This section shows a table of received routes. The columns include Address Family, VPN ID, Prefix, From Peer, Path Id, Label, Status, and Attribute Type. The data shows multiple entries for ipv4 and various prefixes from different peers.
- WAN - Tunnel:** This section includes a line chart showing Loss Percentage and FEC Loss Recovery Rate over time (Real Time, 1h, 3h, 6h, 12h, 24h, 7days, Custom). The legend identifies several tunnels: S100-CE1-private1-DC1-VE1:default[IPSEC], S100-CE1-private1-DC1-VE1:private1[IPSEC], S100-CE1:private1-S200-CE1:private1[IPSEC], S100-CE1:private1-S200-CE1:public-internet[IPSEC], and S100-CE1:public-internet-DC1-VE1:private1[IPSEC]. The chart shows significant fluctuations in loss percentage, particularly for the first two tunnels.



Set up the CA

Root Certificate Authority (CA) สำหรับ Cisco SD-WAN ที่ใช้ X.509 certificates เป็นกลไกความเชื่อถือ (Trust Model) อุปกรณ์ใด ๆ ใน SD-WAN fabric จะต้องมีใบรับรองที่ถูกต้องติดตั้งไว้ มิฉะนั้นจะไม่สามารถเข้าร่วมเครือข่ายได้

```
sudo -i
ip addr add 10.0.0.10/24 dev eth0 || true
ip route add default via 10.0.0.1 || true
grep -qxF 'PermitRootLogin yes' /etc/ssh/sshd_config || echo 'PermitRootLogin yes' >> /etc/ssh/sshd_config
sudo systemctl restart ssh.service
passwd root (ตั้งรหัสผ่าน)
```



```
[root@kali]# sudo systemctl restart ssh.service
[root@kali]# passwd root
New password:
Retype new password:
passwd: password updated successfully
[root@kali]#
```

```
openssl genrsa -out SDWAN.key 2048
openssl req -new -x509 -days 2000 -key SDWAN.key -out SDWAN.pem -sha256 \
-subj "/C=TH/ST=Bangkok/L=Bangkok/O=supawit-lab/CN=supawit"
```

```
[root@kali]# openssl genrsa -out SDWAN.key 2048
[root@kali]# openssl req -new -x509 -days 2000 -key SDWAN.key -out SDWAN.pem -sha256 -subj "/C=TH/ST=Bangkok/L=Bangkok/O=supawit-lab/CN=supawit"
[root@kali]#
```

Set up the DC1-SW1

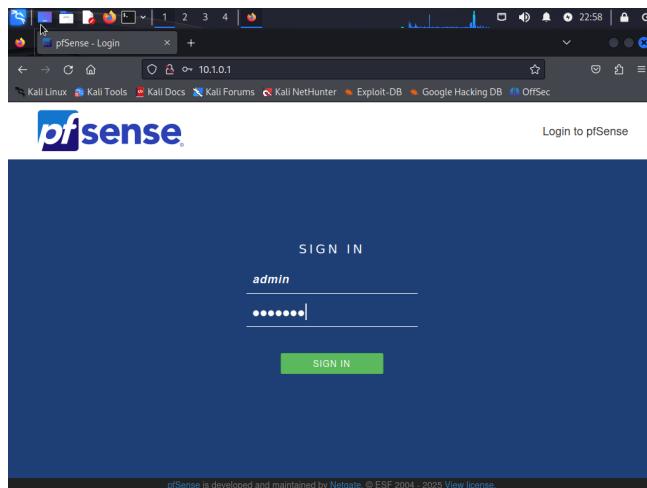
```

hostname DC1-SW1
no ip domain-lookup
!
!
interface Ethernet0/0
no switchport
ip address 10.1.0.2 255.255.255.252
!
interface Ethernet0/1
no switchport
ip address 10.1.1.1 255.255.255.252
!
interface Vlan1
ip address 10.0.0.1 255.255.255.0
no shut
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
!
!
end

```

Set up the Firewall

เนื่องจากในแล็บนี้เราไฟกัสที่ SDN จึงไม่ได้สอน setup firewall แบบละเอียด หรือเราจะใช้ Router มาแทนหน้าที่ได้ (admin:pfsense)



Interfaces Assignment

Interface	Network port
WAN1	vtнет2 (50:00:00:01:00:02)
LAN	vtнет0 (50:00:00:01:00:00)
DMZ	vtнет1 (50:00:00:01:00:01)
WAN2	vtнет3 (50:00:00:01:00:03)

Note:
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.

System Information		
Name	pfSense.home.arpa	
User	admin@10.0.0.10 (Local Database)	
System	QEMU Guest Netgate Device ID: 61cfdf9f253e5f868209f	
BIOS	Vendor: SeaBIOS Version: rel-1.11.1-0-g0551a4be2c-prebuilt.qemu-project.org Release Date: Tue Apr 1 2014	
Version	2.7.1-RELEASE (amd64) built on Wed Nov 15 17:06:00 UTC 2023 FreeBSD 14.0-CURRENT	

Netgate Services And Support		
Retrieving support information		

Interfaces		
WAN1	10Gbase-T <full-duplex>	198.51.100.2
LAN	10Gbase-T <full-duplex>	10.1.0.1
DMZ	10Gbase-T <full-duplex>	10.10.0.1
WAN2	10Gbase-T <full-duplex>	203.0.113.2

Routing Config

pfSense COMMUNITY EDITION

System / Routing / Gateways

Gateways

Name	Default	Interface	Gateway	Monitor IP	Description	Actions	
ISP1	<input checked="" type="checkbox"/>	Tier 1 (IPv4)	WAN1	198.51.100.1	198.51.100.1		
WAN1_DHCP6	<input checked="" type="checkbox"/>		WAN1		Interface WAN1_DHCP6 Gateway		
To_DC1_SW1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN	10.1.0.2	10.1.0.2	To Lan	
ISP2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tier 1 (IPv4)	WAN2	203.0.113.1	203.0.113.1	

Save Add

Default gateway

Default gateway IPv4	WAN ()
Select a gateway or failover gateway group to use as the default gateway.	
Default gateway IPv6	Automatic
Select a gateway or failover gateway group to use as the default gateway.	

Save

pfSense COMMUNITY EDITION

System / Routing / Static Routes

Static Routes

Network	Gateway	Interface	Description	Actions
10.0.0.0/24	To_DC1_SW1 - 10.1.0.2	LAN		
10.1.1.0/30	To_DC1_SW1 - 10.1.0.2	LAN		

Add

System / Routing / Gateway Groups

Gateway Groups

Group Name	Gateways	Priority	Description	Actions
WAN	ISP1 ISP2	Tier 1 Tier 1		

Add

Policy Config (ในที่นี่ allow ทุกอย่าง เพื่อให้ง่ายในการศึกษาแล้วบัน)

Firewall / Rules / WAN1

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	*	*	*	*	*	*	none		

Rules (Drag to Change Order)

Firewall / Rules / LAN

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
2/1.41 MIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
0/672 B	IPv4 *	*	*	*	*	*	*	none		

Rules (Drag to Change Order)

Firewall / Rules / DMZ

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1/8 Kib	IPv4 *	*	*	*	*	*	*	none		

Rules (Drag to Change Order)

Firewall / Rules / WAN2

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	*	*	*	*	*	*	none		

Set up the ISP1

```
hostname ISP1
no ip domain lookup
!
interface Ethernet0/0
ip address 198.51.100.1 255.255.255.252
no shut
interface Ethernet0/1
ip address 198.51.100.5 255.255.255.252
no shut
!
interface Ethernet0/2
ip address 192.0.2.1 255.255.255.252
no shut
!
interface Ethernet0/3
ip address 198.51.100.9 255.255.255.252
no shut
!
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
!
!
ip route 10.0.0.0 255.0.0.0 198.51.100.2
ip route 10.0.0.0 255.0.0.0 192.0.2.2 5
!
end
```

Set up the ISP2

```
hostname ISP2
no ip domain lookup
!
interface Ethernet0/0
ip address 203.0.113.1 255.255.255.252
no shut
!
interface Ethernet0/1
ip address 203.0.113.9 255.255.255.252
no shut
!
interface Ethernet0/2
ip address 192.0.2.2 255.255.255.252
no shut
```

```
!
interface Ethernet0/3
 ip address 203.0.113.5 255.255.255.252
no shut
!
router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
!
ip forward-protocol nd
!
!
ip route 10.0.0.0 255.0.0.0 203.0.113.2
ip route 10.0.0.0 255.0.0.0 192.0.2.1 5
!
end
```

Set up the vBond

```
conf t
system
host-name vBond
system-ip 10.10.0.4
site-id 10000
organization-name supawit-lab
vbond 10.10.0.3 local vbond-only
!
vpn 0
interface ge0/0
ip address 10.10.0.3/24
no tunnel-interface
no shutdown
ip route 0.0.0.0/0 10.10.0.1
!
commit and-quit

vshell
scp root@10.0.0.10:SDWAN.pem .
exit

request root-cert-chain install /home/admin/SDWAN.pem
```

- ค่าที่ตั้งใน organization-name ต้องตรงกับที่ใช้ใน PnP vBond profile และต้องเหมือนกันทุกอุปกรณ์ใน SD-WAN Fabric
- อุปกรณ์ทุกตัวใน Fabric ต้องรู้ว่าเข้าถึง vBond
- ไฟล์ vBond image ใช้ไฟล์เดียวกันกับ vEdge Cloud แต่การตั้งค่า vbond-only บน VM จะทำให้ระบบรู้ว่าอุปกรณ์นี้ทำหน้าที่เป็น vBond

ความหมายของ VPN ใน Cisco SD-WAN

- VPN ใน Cisco SD-WAN คล้ายกับ VRF (Virtual Routing and Forwarding)
- VPNO คือ Transport VPN ที่ใช้กับทุกอุปกรณ์ใน SD-WAN
- Static Route ที่กำหนด ใช้ได้เฉพาะใน VPNO
- IPsec / GRE Tunnels จะถูกสร้างขึ้นบน VPNO
- การตั้งค่า ‘skinny’ configuration ปิดการทำงานของ VPNO Tunnel Interface ชั่วคราว จนกว่าจะตั้งค่า vSmart และ vManage เสร็จ เพื่อหลีกเลี่ยงปัญหา “ໄກกับไฟ” (ปัญหาการเชื่อมต่อและความเชื่อถือของ Certificate)

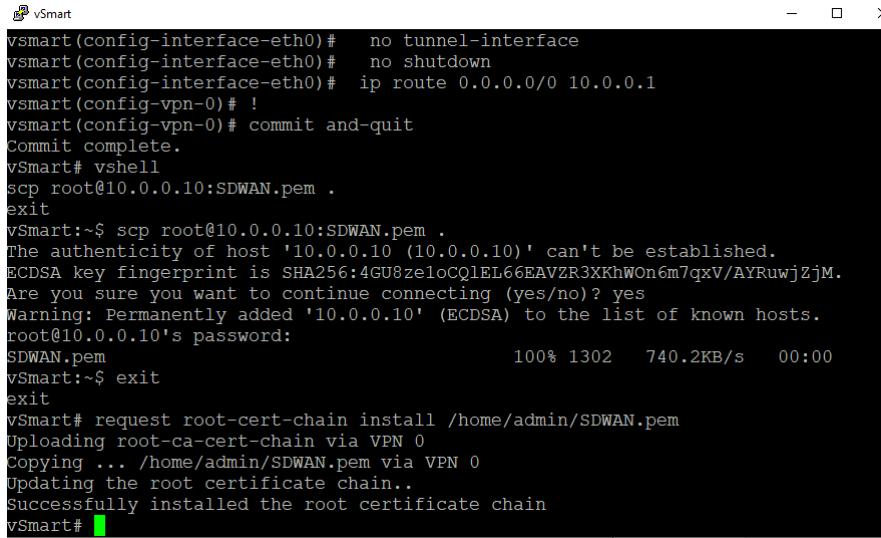
```
vBond# vsh
vBond:~$ scp root@10.0.0.10:SDWAN.pem .
root@10.0.0.10's password:
SDWAN.pem                                         100% 1302      62.2KB/s   00:00
vBond:~$ exit
exit
vBond# request root-cert-chain install /home/admin/SDWAN.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/SDWAN.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
vBond#
```

Set up the vSmart

```
conf t
system
host-name vSmart
system-ip 10.0.0.201
site-id 10000
organization-name supawit-lab
vbond 10.10.0.3
!
vpn 0
interface eth0
ip address 10.0.0.200/24
no tunnel-interface
no shutdown
ip route 0.0.0.0/0 10.0.0.1
!
commit and-quit

vshell
scp root@10.0.0.10:SDWAN.pem .
exit

request root-cert-chain install /home/admin/SDWAN.pem
```



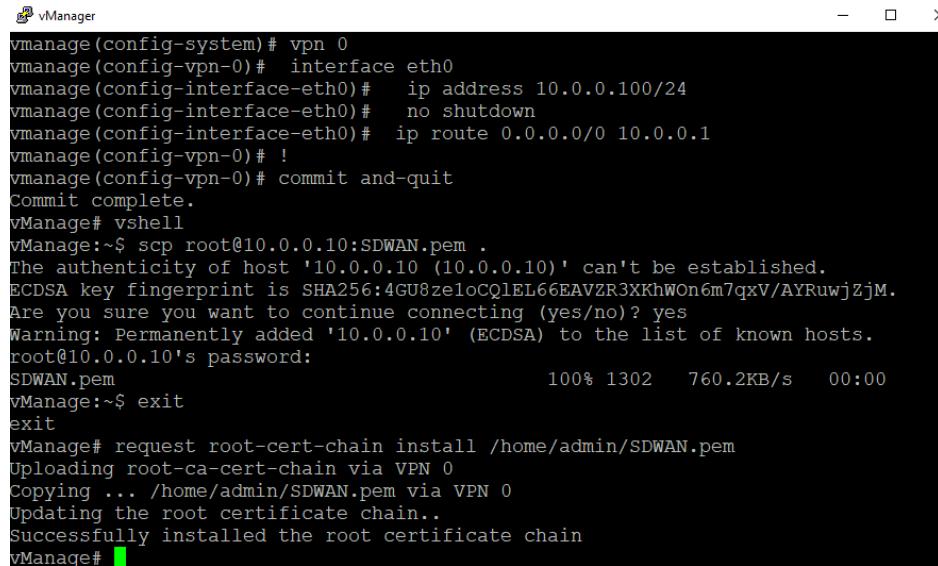
```
vSmart# no tunnel-interface
vSmart# no shutdown
vSmart# ip route 0.0.0.0/0 10.0.0.1
vSmart# !
vSmart# commit and-quit
Commit complete.
vSmart# vshell
scp root@10.0.0.10:SDWAN.pem .
exit
vSmart:~$ scp root@10.0.0.10:SDWAN.pem .
The authenticity of host '10.0.0.10 (10.0.0.10)' can't be established.
ECDSA key fingerprint is SHA256:4GU8ze1oCQ1EL66EAVZR3XKhWOn6m7qxV/AYRuwjZjM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.10' (ECDSA) to the list of known hosts.
root@10.0.0.10's password:
SDWAN.pem
100% 1302 740.2KB/s 00:00
vSmart:~$ exit
exit
vSmart# request root-cert-chain install /home/admin/SDWAN.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/SDWAN.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain.
vSmart#
```

Set up the vManage

```
conf t
system
host-name vManage
system-ip 10.0.0.101
site-id 10000
organization-name supawit-lab
vbond 10.10.0.3
!
vpn 0
interface eth0
ip address 10.0.0.100/24
no shutdown
ip route 0.0.0.0/0 10.0.0.1
!
commit and-quit

vshell
scp root@10.0.0.10:SDWAN.pem .
exit

request root-cert-chain install /home/admin/SDWAN.pem
```



```

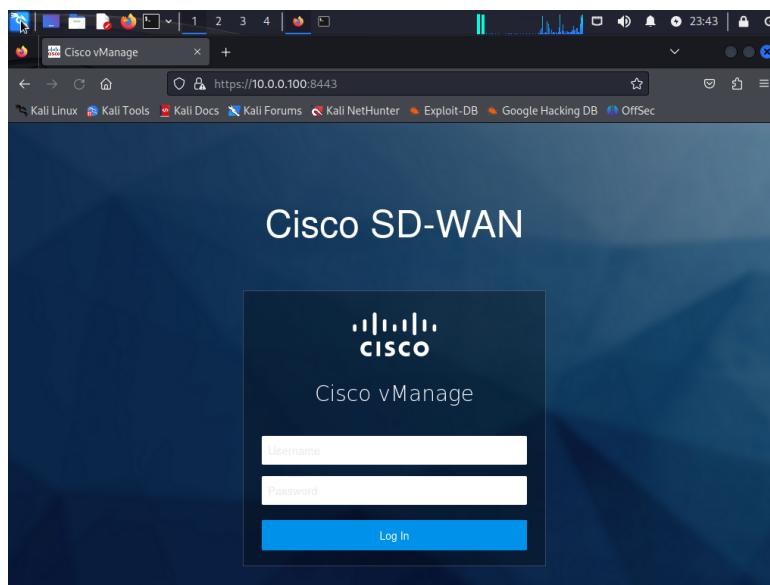
vManager# vpn 0
vManage(config-system)# interface eth0
vManage(config-interface-eth0)# ip address 10.0.0.100/24
vManage(config-interface-eth0)# no shutdown
vManage(config-interface-eth0)# ip route 0.0.0.0/0 10.0.0.1
vManage(config-vpn-0)# !
vManage(config-vpn-0)# commit and-quit
Commit complete.
vManage# vshell
vManage:~$ scp root@10.0.0.10:SDWAN.pem .
The authenticity of host '10.0.0.10 (10.0.0.10)' can't be established.
ECDSA key fingerprint is SHA256:4GU8ze1oCQ1EL66EAVZR3XKhWOn6m7qxV/AYRuwjZjM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.10' (ECDSA) to the list of known hosts.
root@10.0.0.10's password:
SDWAN.pem                                         100% 1302    760.2KB/s   00:00
vManage:~$ exit
vManage# request root-cert-chain install /home/admin/SDWAN.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/SDWAN.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
vManage#

```

ตอนนี้ให้ใช้ เว็บเบราว์เซอร์ (จากเครื่อง CA ในแล็บนี้ และสำหรับตัวอย่างทั้งหมดต่อจากนี้) เพื่อเข้าสู่ vManage Web Console ที่

<https://10.0.0.100:8443>

หมายเหตุ: หาก VM เพิ่งรีบูต อาจต้องรอสักครู่ก่อนที่ Web Interface จะพร้อมใช้งาน



เมื่อเข้าใช้งาน vManage ครั้งแรก ระบบจะแสดง คำเตือนเกี่ยวกับ Self-Signed Certificate ซึ่งสามารถเพิกเฉยได้ เมื่อจากเป็นแค่คือทดสอบ
เข้าสู่ระบบด้วย: admin / admin
ตั้งค่าบน vManage

1. ไปที่ Administration > Settings
2. แก้ไขค่า Organization Name ให้ตรงกับค่าที่ตั้งไว้ในอุปกรณ์อื่น ๆ (supawit-lab)

3. แก้ไขค่า vBond และระบุ vBond Address
4. ตั้งค่า Controller Certificate Authorization เป็น Manual (เนื่องจากแล็บนี้ใช้ Self-Signed Certificates หากใช้ PKI (Public Key Infrastructure) ขององค์กรที่มี CA Hierarchy สามารถเลือก Enterprise Root Certificate ได้แทน)

The screenshot shows the Cisco vManage Administration Settings page. The 'Controller Certificate Authorization' section is highlighted with a red box. Other sections shown include Organization Name (supawit-lab), vBond (10.10.0.3 : 12346), Email Notifications (Disabled), Hardware WAN Edge Certificate Authorization (Onbox), and WAN Edge Cloud Certificate Authorization (Automated).

Organization Name	supawit-lab	View Edit
vBond	10.10.0.3 : 12346	View Edit
Email Notifications	Disabled	View Edit
Hardware WAN Edge Certificate Authorization	Onbox	View Edit
Controller Certificate Authorization	Manual	View Edit
WAN Edge Cloud Certificate Authorization	Automated	View Edit
Web Server Certificate	12 Jul 2024 6:30:30 PM	CSR Certificate
Enforce Software Version (ZTP)		View Edit
Banner	Disabled	View Edit
Reverse Proxy	Disabled	View Edit
Statistics Setting		View Edit

Prepare the controller certificates

เพิ่ม vBond และ vSmart บน vManage

ไปที่ vManage และทำตามขั้นตอนนี้

1. ไปที่ Configuration > Devices > Controllers > Add Controller > vBond

The screenshot shows the Cisco vManage Configuration | Devices page with the 'Controllers' tab selected. A table lists a single vBond entry: Controller Type (vManage), Hostname (vManage), System IP (10.0.0.101), Site ID (10000), Mode (CLI), Assigned Template (–), and Device Status (In Sync). The 'Add Controller' button is visible at the top left.

Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status
vManage	vManage	10.0.0.101	10000	CLI	–	In Sync

2. ป้อน vBond IP Address ที่ใช้กำหนดไว้ทุกที่ (ในตัวอย่างนี้คือ 10.10.0.3)
3. ป้อน admin username และ password
4. ยกเลิกการเลือก "Generate CSR"

5. ทำการขึ้นตอนเดียวกันเพื่อเพิ่ม vSmart Controller (ใช้ IP 10.0.0.200)
6. ใช้ค่า Protocol เป็นค่าเริ่มต้น (DTLS) และยัง ไม่ต้องสร้าง CSR

Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status
vManage	vManage	10.0.0.101	10000	CLI	--	In Sync ***
vSmart	--	--	--	CLI	--	***
vBond	--	--	--	CLI	--	***

สร้าง CSR (Certificate Signing Request)

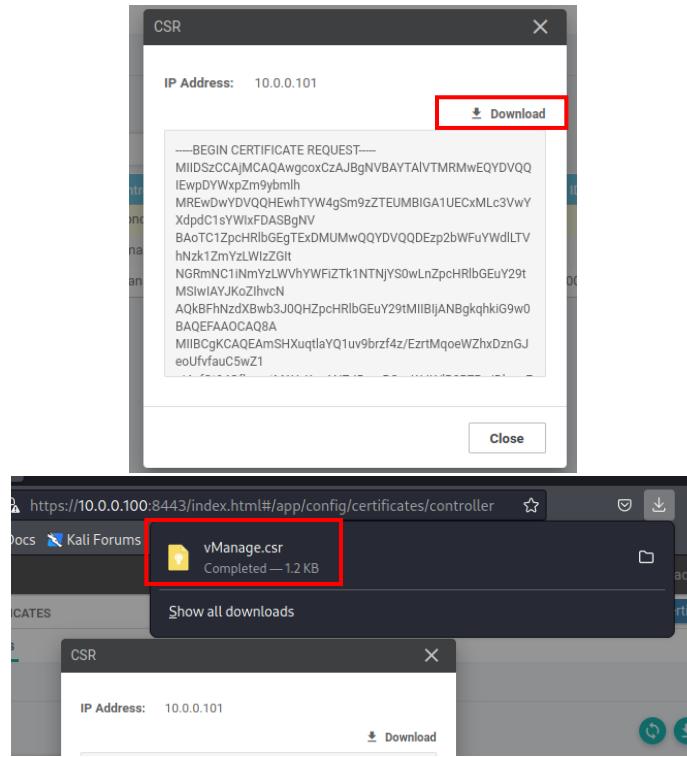
1. ไปที่ Configuration > Certificates > Controllers

2. สำหรับแต่ละ Controller คลิก จุดสามจุด ทางขวา แล้วเลือก Generate CSR

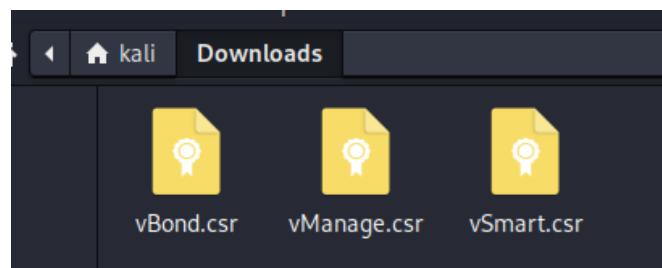
Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate
N/A	vBond	--	--	--	No certificate installed ***
N/A	vSmart	--	--	--	No certificate installed ***
N/A	vManage	vManage	10.0.0.101	10000	No certificate installed ***

3. ดาวน์โหลดไฟล์ CSR ของแต่ละอุปกรณ์ และเปลี่ยนชื่อเป็น:

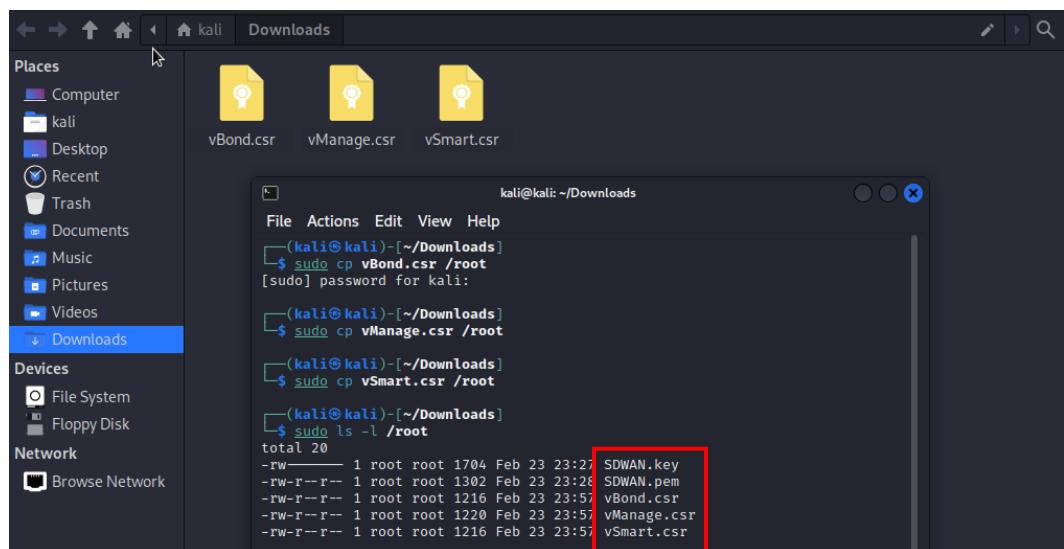
- a. vManage.csr



- b. vBond.csr
- c. vSmart.csr



4. ย้ายไฟล์เหล่านี้ไปยังโฟลเดอร์เดียวกันกับ Root Key และ Root Certificate บน CA Machine



สร้างและเข็นใบรับรองอุปกรณ์ (Device Certificates)

ใช้คำสั่งต่อไปนี้บน CA Machine เพื่อลงนาม (sign) ใบรับรองแต่ละตัว

```
openssl x509 -req -in vManage.csr -CA SDWAN.pem -CAkey SDWAN.key \
-CAcreateserial -out vManage.pem -days 2000 -sha256

openssl x509 -req -in vBond.csr -CA SDWAN.pem -CAkey SDWAN.key \
-CAcreateserial -out vBond.pem -days 2000 -sha256

openssl x509 -req -in vSmart.csr -CA SDWAN.pem -CAkey SDWAN.key \
-CAcreateserial -out vSmart.pem -days 2000 -sha256
```

```
(kali㉿kali)-[~/Downloads]
$ sudo -i
(root㉿kali)-[~]
# openssl x509 -req -in vManage.csr -CA SDWAN.pem -CAkey SDWAN.key -CAcreateserial -out vManage.pem -days 2000 -sha256
Certificate request self-signature ok
subject=C = US, ST = California, L = San Jose, OU = supawit-lab, O = Viptela LLC, CN = vmanage-5a795ff3-b3db-4df4-b6f3-eaaabe9553ca-0.viptela.com, emailAddress = support@viptela.com

(root㉿kali)-[~]
# openssl x509 -req -in vBond.csr -CA SDWAN.pem -CAkey SDWAN.key -CAcreateserial -out vBond.pem -days 2000 -sha256
Certificate request self-signature ok
subject=C = US, ST = California, L = San Jose, OU = supawit-lab, O = Viptela LLC, CN = vbond-6430a83b-1b17-49e0-990e-e8e4fbdbb3a3-0.viptela.com, emailAddress = support@viptela.com

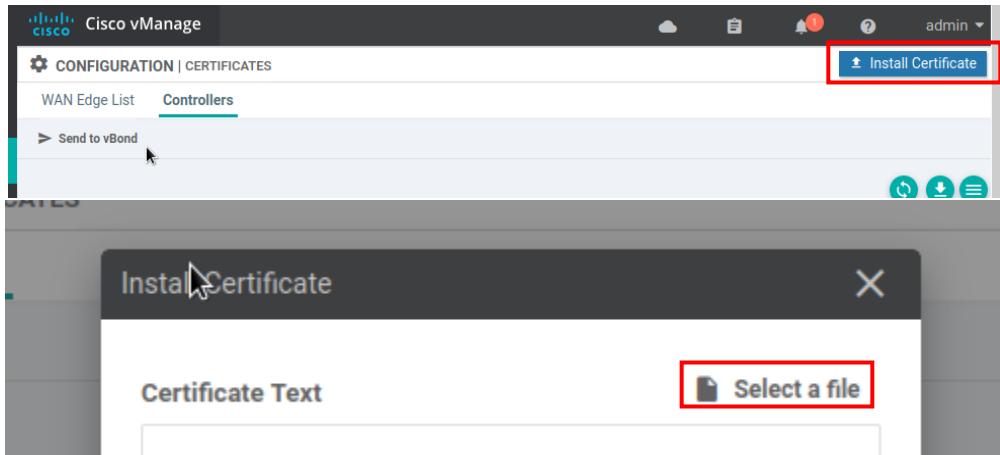
(root㉿kali)-[~]
# openssl x509 -req -in vSmart.csr -CA SDWAN.pem -CAkey SDWAN.key -CAcreateserial -out vSmart.pem -days 2000 -sha256
Certificate request self-signature ok
subject=C = US, ST = California, L = San Jose, OU = supawit-lab, O = Viptela
```

คัดลอกกลับไปยัง Downloads

```
(root㉿kali)-[~]
# cp vSmart.pem /home/kali/Downloads
(root㉿kali)-[~]
# cp vBond.pem /home/kali/Downloads
(root㉿kali)-[~]
# cp vManage.pem /home/kali/Downloads
(root㉿kali)-[~]
```

ติดตั้งใบรับรองบน vManage

1. ไปที่ Configuration > Certificates > Controllers
2. คลิก Install Certificate ที่มุ่งหมาย



3. ติดตั้งไฟล์ Certificate ที่สำเนาตัว
 - a. vManage.pem
 - b. vBond.pem
 - c. vSmart.pem
4. หลังจากติดตั้งสำเร็จ กลับไปที่หน้า Controller Certificate Configuration
5. ตรวจสอบว่า Certificate Serial Number ของแต่ละอุปกรณ์ปรากฏขึ้นแล้ว

	Controller Type	Hostname	Certificate Serial	Operation Status	System IP	Expiration Date	uu	...
>	vBond	--	0C1914FB5B1817543FD6...	Installed	--	17 Aug 2030 1:02:12 ...	64	***
>	vSmart	--	0C1914FB5B1817543FD6...	vBond Updated	--	17 Aug 2030 1:02:25 ...	58	***
>	vManage	vManage	0C1914FB5B1817543FD6...	vBond Updated	10.0.0.101	17 Aug 2030 1:01:56 ...	5a	***

เปิดใช้งาน VPN0 Tunnel Interface บน SD-WAN Controllers

เปิดใช้งาน Tunnel บน vManage และ vSmart

ให้ล็อกอินเข้า Console ของ vManage และ vSmart และป้อนคำสั่งนี้:

```
conf t
vpn 0
interface eth0
  tunnel-interface
commit and-quit
```

ล็อกอินเข้า Console ของ vBond และป้อนคำสั่งนี้:

```

conf t
vpn 0
interface ge0/0
tunnel-interface
encapsulation ipsec
commit and-quit

```

หลังจากตั้งค่าเสร็จ Dashboard จะอัปเดตเพื่อแสดงสถานะการเชื่อมต่อใหม่

ตรวจสอบการเชื่อมต่อเพิ่มเติม

ไปที่ Monitor > Network และตรวจสอบว่า ทั้งสาม Controllers (vManage, vSmart, vBond) แสดงสถานะ "reachable"

The screenshot shows the Cisco vManage Main Dashboard. It features a top navigation bar with tabs like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation is a header with the Cisco vManage logo and a user dropdown for 'admin'. The main area is titled 'DASHBOARD | MAIN DASHBOARD' and includes several key metrics:

- Control Status (Total 0):** Control Up (0), Partial (0), Control Down (0).
- Site Health (Total 0):** Full WAN Connectivity (0 sites), Partial WAN Connectivity (0 sites), No WAN Connectivity (0 sites).
- Transport Interface Distribution:** Categories include < 10 Mbps (0), 10 Mbps - 100 Mbps (0), 100 Mbps - 500 Mbps (0), and > 500 Mbps (0).

The screenshot shows the Cisco vManage MONITOR | NETWORK page under the 'WAN - Edge' tab. The left sidebar has icons for Home, Devices, Monitoring, Security, and Scripts. The main content area displays a table of devices:

Hostname	State	System IP	Reachability	Site ID	Device Model	BFD	Control	Version
vManage	reachable	10.0.0.101	reachable	10000	vManage	-	1	19.2.0
vSmart	reachable	10.0.0.201	reachable	10000	vSmart	-	1	19.2.097
vBond	reachable	10.10.0.4	reachable	10000	vEdge Cloud (vBo...)	-	-	19.2.0

cEdge01 (S100-CE1)

การนำอุปกรณ์ cEdge เข้าสู่ SD-WAN Fabric สำหรับ Site 100 ให้ล็อกอินเข้า Console ของ cEdge และเพิ่มการตั้งค่าเริ่มต้น

```
config-transaction
!
hostname S100-CE1
username admin priv 15 secret admin
no ip domain lookup
!
system
system-ip 10.100.10.2
site-id 100
organization-name supawit-lab
vbond 10.10.0.3
exit
!
ip route 0.0.0.0 0.0.0.0 198.51.100.5
ip route 0.0.0.0 0.0.0.0 203.0.113.5
interface GigabitEthernet1
no shutdown
ip address 198.51.100.6 255.255.255.252
interface GigabitEthernet2
no shutdown
ip address 203.0.113.6 255.255.255.252
!
commit
end
```

```

Router(config)# ip route 0.0.0.0 0.0.0.0 198.51.100.5
Router(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.5
Router(config)# interface GigabitEthernet1
Router(config-if)# no shutdown
Router(config-if)# ip address 198.51.100.6 255.255.255.252
Router(config-if)# interface GigabitEthernet2
Router(config-if)# no shutdown
Router(config-if)# ip address 203.0.113.6 255.255.255.252
Router(config-if)#
Router(config-if)#
Router(config-if)#
*Feb 24 05:20:00.972: %AAAAA-4-CLI_DEPRECATED: WARNING: Command has been added to
the configuration using a type 5 password. However, type 5 passwords will soon
be deprecated. Migrate to a supported password typeCommit complete.
S100-CE1(config-if)#
Uncommitted changes found, commit them? [yes/no/CANCEL]
*Feb 24 05:20:01.273: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF
ONF by admin, transaction-id 197
*Feb 24 05:20:01.404: %Cisco-SDWAN-Router-OMP-5-NTCE-400003: R0/0: OMPD: Operational state changed to UP
*Feb 24 05:20:01.723: %OSPF-6-DFT_OPT: Protocol timers for fast convergence are
Enabled.
Aborted: by user
S100-CE1(config)#

```

เนื่องจาก Router นี้ไม่ compatible ในเรื่อง key ssh กับตัว CA จึงต้องต้องใช้วิธีที่ขั้นตอนเล็กน้อย

```

S100-CE1#copy scp://root@10.0.0.10:/SDWAN.pem bootflash:
Destination filename [SDWAN.pem]?
%Error opening scp://@10.0.0.10/SDWAN.pem (Undefined error)
S100-CE1#
*Feb 24 05:24:44.666: %SSH-3-NO_MATCH: No matching kex algorithm found: client diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1 server sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256
S100-CE1#

```

ไปที่ vManage cli

- เบิดไฟล์ SDWAN.pem ด้วย cat

```

vManage# vsh
vManage:~$ cat SDWAN.pem
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIUFmx2ghcHw+Rm6/H0ZJBx8urLBWEwDQYJKoZIhvcNAQEL
BQAwwTELMAkGA1UEBhMCVEgxEADOBgNVBAgMB0Jhbmdrb2sxEDAOBgNVBAcMB0Jh
bmdrb2sxFDASBqNVBAoMC3N1cGF3aXQtbGFiMRAwDgYDVQQDAzdXhd210MB4X
DTI1MDIyNDA0Mjg1MF0xDTMwMDgxNzA0Mjg1MFowTTELMAkGA1UEBhMCVEgxEADo
BgNVBAgMB0Jhbmdrb2sxEDAOBgNVBAcMB0Jhbmdrb2sxFDASBqNVBAoMC3N1cGF3
aXQtbGFiMRAwDgYDVQDADzXhd210MIBIjANBgkqhkiG9wOBAQEFAAOCAQ8AM
MIIBCgKCAQEAm5NwDckAm+H6cV8q4Cchd/DNuqv9cVKb5zDvVDLH/VgFZKgBCjz
CKQCAjI4prZaDLNTsV3pxv9wAf4db/isVn3NnY9w+Qh0Tiq912izJn8HAHFianR
cudt1PnftYtAkUgMlnCA0ufUQqdfpcsn_9JF+3PAJiaMfkwhn3Dr6sMJ0u7WrD
DleTeAHgRmqa1QuW6Wz5jPQcePULkcvA3Vkd2dk1oKWyPVPWbfU53+UunC2PIyc
U0UKnyEGeAdoP1N8bOYZks3hZYFPapNjJvHpozW1DtLbmO95IeJ/p80vNDHtQ1YRe
WMS+8Cbz1CP9SDhEyGBF8I+RCDuPqW+02WIDAQABoIMwUTAdBgNVHQ4EFgQUkjKE
tso5pv6msWRQzowExeafKZMwHwYDVR0jBgvwPoAUkjEtso5pv6msWRQzowExeaf
KZMwDwYDVR0TAQh/BAUwAwEB/zANBgkqhkiG9wOBAQsFAAOCAQEzdmvMOFZgGZ
NKzPReUoTjopvYwmMPgyvk/c1nh5H6S9/PuPU+wHfLohbB5XESz70+MuAQdsAgNq
4sEUJthcB3iZBS1uPJS3dnD6bHnaT216G+HTsvJTX8v+OV3w70c8HmGdxFowmeqO
dhDu8fV897DfsiwiXG9/jkxr1qiyqto+jtvte8k3zhFP11G1RUyH9t39L5Fr/9t
Tg1v7r5iZGu9vGWNetqNoc0WA5LqTNM9M//d6tEwh36rlbLtw7onBTS4EKp6fpa
EyIMsGSXvogg3nsK38fwYWGseIceuNvtqoS2+z248g9CtelucysxdwTFkbrjYK1
9KkYZ/w70A=-
-----END CERTIFICATE-----
vManage:~$ 

```

2. งานนี้ copy เนื้อหาทั้งหมดใส่ใน format นี้ แล้ววางไว้ใน Notepad

```
tclsh
set f [open "bootflash:SDWAN.pem" w]
puts $f {----BEGIN CERTIFICATE----
(แทนที่ Key)
----END CERTIFICATE----}
close $f
```



```
*simple_cEdge.txt - Notepad
File Edit Format View Help
tclsh
set f [open "bootflash:SDWAN.pem" w]
puts $f {----BEGIN CERTIFICATE----
MIIDkzCCAnugAwIBAgIUFmx2ghCHw-Rm6/H0zJBx8urLBWEwDQYJKoZIhvcNAQEL
BQAwNTELMAkGA1UEBhMCVEgxEDAObgNVBAgMB0Jhbmdrb2sxEDAObgNVBAcMB0Jh
bmdrb2sxFDASBgNVBAoMC3N1cGF3aXQtbgF1MRAwDgYDVQDDAdzdBhd2l0MB4X
DTI1MDIyNDA0Mjg1MFoXTDMwMDgxNzA0Mjg1MFowNTELMAkGA1UEBhMCVEgxEDA
BgNVBAgMB0Jhbmdrb2sxEDAObgNVBAcMB0Jhbmdrb2sxFDASBgNVBAoMC3N1cGF3
aXQtbgF1MRAwDgYDVQDDAdzdBhd2l0MITBIjANBgkqhkiG9w0BAQEAAQCAQ8A
MIIBCgKCAQEAm5NwDckAm+H6oV8q4CchD/DNuqv9cVKb5rDvVDHL/H/fGZKqBcjz
CKQCAj4prZaDLNTsV3pzxv9Af4db/isVn3NnY9w+Qh0Tlq912izJn8HAHFianR
cudt1PnftY+tAkuGmLmCA0ufUQqdfpcJn/9JF+3PAJiaMfkwhn3Dr6sMJ0u7WrD
DleTeAHgRmqa0lQv6Wz5jPQcePULkcvA3Vkd2dkioWKYPVWbfu53+UunC2Piyc
U0UKnYEGeA0PlN8bOYZks3hZFYapNjVhpzW1DtLbm095IeJ/p80vNDHtQlYRe
WMS+8Cbz1CP9SDhEyGBF8I+RCDUPqW+02wIDAQABoIMwUTAdBgNVHQ4EfgrQujkE
ts0s5pv6msWRQzowExeafkZMuHwYDVR0jB8gwfoAUkjkEtso5pv6msWRQzowExeaf
KZMwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAdmNvMOfZgGZ
NKzPREutojOpvYwmMPgyvk/c1nh5HS9/PuPU+wHfLohb5XESz70+MuAQdsAgNg
4sEUJthcB3iZBS1uPJS3dnD6bHtaT216G+HTSvJTX8V+oV3w70c8HmGdXFowmeqO
dhDu8fV897DfsiwiXg9/jkxr1qiyqt0+JtvIE8k3zhFP1jG1RUYh9139L5Fr/9t
Tg1v75iZgu9GWNNetqNOc0WA5LqTNM9M/d6tEwh36rLbLtw7onBTS4EKp6fp
EyIMsGSXvogg3nsK38fWYWGseIceuNvtqo052+z248g9Cte1ucySxdwTFkbrjYK1
9KKYZ/w70A==
----END CERTIFICATE----}
close $f
```

3. Copy คำเนื้อหาทั้งหมด ไปวางให้กับ cEdge

```
S100-CE1>
S100-CE1>ena
S100-CE1>tclsh
S100-CE1(tcl)*#set f [open "bootflash:SDWAN.pem" w]
file10
S100-CE1(tcl)*#puts $f {----BEGIN CERTIFICATE----
+MIIDkzCCAnugAwIBAgIUFmx2ghCHw-Rm6/H0zJBx8urLBWEwDQYJKoZIhvcNAQEL
+BQAwNTELMAkGA1UEBhMCVEgxEDAObgNVBAgMB0Jhbmdrb2sxEDAObgNVBAcMB0Jh
+>bmdrb2sxFDASBgNVBAoMC3N1cGF3aXQtbgF1MRAwDgYDVQDDAdzdBhd2l0MB4X
+>DTI1MDIyNDA0Mjg1MFoXTDMwMDgxNzA0Mjg1MFowNTELMAkGA1UEBhMCVEgxEDA
+>BgNVBAgMB0Jhbmdrb2sxEDAObgNVBAcMB0Jhbmdrb2sxFDASBgNVBAoMC3N1cGF3
+>aXQtbgF1MRAwDgYDVQDDAdzdBhd2l0MITBIjANBgkqhkiG9w0BAQEAAQCAQ8A
+>MIIBCgKCAQEAm5NwDckAm+H6oV8q4CchD/DNuqv9cVKb5rDvVDHL/H/fGZKqBcjz
+>CKQCAj4prZaDLNTsV3pzxv9Af4db/isVn3NnY9w+Qh0Tlq912izJn8HAHFianR
+>cudt1PnftY+tAkuGmLmCA0ufUQqdfpcJn/9JF+3PAJiaMfkwhn3Dr6sMJ0u7WrD
+>DleTeAHgRmqa0lQv6Wz5jPQcePULkcvA3Vkd2dkioWKYPVWbfu53+UunC2Piyc
+>U0UKnYEGeA0PlN8bOYZks3hZFYapNjVhpzW1DtLbm095IeJ/p80vNDHtQlYRe
+>WMS+8Cbz1CP9SDhEyGBF8I+RCDUPqW+02wIDAQABoIMwUTAdBgNVHQ4EfgrQujkE
+>ts0s5pv6msWRQzowExeafkZMuHwYDVR0jB8gwfoAUkjkEtso5pv6msWRQzowExeaf
+>KZMwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAdmNvMOfZgGZ
+>NKzPREutojOpvYwmMPgyvk/c1nh5HS9/PuPU+wHfLohb5XESz70+MuAQdsAgNg
+>4sEUJthcB3iZBS1uPJS3dnD6bHtaT216G+HTSvJTX8V+oV3w70c8HmGdXFowmeqO
+>dhDu8fV897DfsiwiXg9/jkxr1qiyqt0+JtvIE8k3zhFP1jG1RUYh9139L5Fr/9t
+>Tg1v75iZgu9GWNNetqNOc0WA5LqTNM9M/d6tEwh36rLbLtw7onBTS4EKp6fp
+>EyIMsGSXvogg3nsK38fWYWGseIceuNvtqo052+z248g9Cte1ucySxdwTFkbrjYK1
+>9KKYZ/w70A==
+>----END CERTIFICATE----}
S100-CE1(tcl)*#close $f
S100-CE1(tcl)*#
```

4. ใช้คำสั่งนี้กับ cEdge

```
request platform software sdwan root-cert-chain install bootflash:SDWAN.pem
request platform software sdwan csr upload bootflash:cedge01_csr (supawit-lab, supawit-lab)
```

```
S100-CE1(tcl) #exit
S100-CE1#
S100-CE1#
S100-CE1#
S100-CE1#$tform software sdwan root-cert-chain install bootflash:SDWAN.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /bootflash/SDWAN.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
S100-CE1#
S100-CE1#
S100-CE1#request platform software sdwan csr upload bootflash:cedge01_csr
Uploading CSR via VPN 0
Enter organization name : supawit-lab
Re-enter organization name : supawit-lab
Generating private/public pair and CSR for this vedge device
Generating CSR for this vedge device .....[DONE]
Copying ... /bootflash/cedge01_csr via VPN 0
CSR upload successful
S100-CE1#
```

5. สร้าง cedge01.csr ที่ vManager ด้วย Vim จากนั้นวางเนื้อหาของ cedge01 ที่อยู่ใน cEdge01 ลงไป

```
vsh
vi cedge01.csr
```

```
S100-CE1#more bootflash:/cedge01_csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDTTCCAJUCAQwgcvxCzAJBgNVBAYTA1VTMRMwEQQYDVQQIBwpDXWxpZm9ybmlh
MREwDwYDVQQHEwhTYW4gSm9zZTEUMBIGA1UECxMLc3VwYXdpdC1sYWIXFDASBgNV
BAoTC3ZJUHRlbGBgSW5jMUUwQwYDVQDEzx2ZWRnZS1DU1ItZTziY2Q3M2EtODhh
Mi00ZjI4LTkwNzUtMW1xOT1kMD11Zjg2LTEudmlwdGVsYS5jb20xiAgBgkqhkiG
9w0BCQEWE3N1cHBvcnRadmlwdGVsYS5jb20wggBiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwgEKAoIBAQDwmsi08XuwCnCyabld3z0OyuZ1Tns/BwO+3dRI/YvDDms2Aw0
e/bPBIRvDmzIGzhiaSpokncoa0TLMQ7022FnPtbdYi1vdWzcibem8ZG4gB0VfUN
jgKxb7woOL6fs1L+jvYwbStp6Tv3mp72/QQDtRb1BgnkNzIGucT1fUS4GUHLtKY
k+Iq5egNpFhxa/nKqVjt6nKHgtPoohG1BxewJPKRcp0ASwvFmZTt0lu+lnVjUYOK
fJ470IPbj7+S1RJ8McChYFmcymbOuyHkJ/g8v106jbc4MnamvG6GQ784BOBptWvI
61F+s1pEG0GQa6M0jOkAwueFcEgqm3lrY81AgMBAAGgOzA5BgkqhkiG9wOBCQ4x
LDAqMAkGA1UDewQCMAAWHQYDVR0OBByEFIphtZGSSqqFTfr7esGzs4bdKk5MA0G
CSqGS1b3DQEBCwUAA4IBAQAJAKHSYdfqht9qL2YZHsZYb5B91GOT8pVkaFCCOZlm
2kyi++1py8cUPoDzYmGxVbcDC53+7iLV7aR6spmdl7YoGDr+XZAxkSLVPDXJj3Ws
tf8vk3zqEnp1gaAGqrRyeOFDNKRSF/bK4uxevpi2ts6iGBzr7lmFI2VsfpA7jkPK
V2F+j9rlxqbYGD3oNyjg4/hzCdjd5v5iWnc82eGYt+arRI5Pm6b7H3vydmfZWKOP
HVuhbUQyyUWrU6kbBYVDDtPM2/U4pqxo55MGqz0kUb7+i4KExyaVe+lg9czSD/wz
Y1dv64IpYo90iQ1VCCSO+M076F3CF5l0y3jcScrqJnMJ
-----END CERTIFICATE REQUEST-----
S100-CE1#
```

```
vManage:~$  
vManage:~$  
vManage:~$ cat cedge01.csr  
-----BEGIN CERTIFICATE REQUEST-----  
MIIDTTCCAjUCAQAwgcwxCzAJBgNVBAYTA1VTMRMwEQQYDVQQIEwpDYWxpZm9ybmlh  
MRkwDwYDVQQHewhTW4gSm9zZTEUMBIGA1UECxMLc3VwYXdpdC1sYWIxFDASBgNV  
BAoTC3ZJUHR1bGEgSW5jMUUwQwYDVQQDEzx2ZWNRnZs1DU1ITZTziY2Q3M2EtODhh  
Mi00Zj14LTkwNzUTMWIxOTlkMDI1Zjg2LTEudmlwdGvsYS5jb20wgE1MA0GCSqGSIb3DQEBAQUAA4IB  
9w0BCQEWE3NlcHBvcnRAdmlwdGvsYS5jb20wgE1MA0GCSqGSIb3DQEBAQUAA4IB  
DwAwggEKAoIBAQDwmsiO8xuwCnCyab1d3z0OyuZ3ITns/Bwo+3dRI/YvdDms2Aw0  
e/bPB1rVDMzIGzbiaSpoknCoa0TLMQ702zFnPtbdYi1VdWzcibem8ZG4gBOVfUN  
jgKxb7woOL6fS1L+jYYwBsTp6Tv3mp7z/QQDtRblBgnkNzIGuct1fUS4GJUHLtKY  
k+1q5egNpFHxa/nKqVjt6nKHGTpoOhGIBXewPkrCp0ASwvFmZTt0lu+lnVjUY0K  
fj470IPbj7+SLRJ8McChYFmcymbouyHkj/g8vi06jbc4MnamvG6GQ784B0BptWvI  
61F+S1pEG0Gqa6M0jokAwuefFcEgQm31rY81AgMBAAggOzA5BqkghkiG9w0BCQ4x  
LDAqMAkGA1UdEwQCMAwHQYDVROOBByFIPthZGSqqqTFtr7esGzvS4bdKk5MA0G  
CSqGS1b3DQEBCWUA41BAQAJAKHSYdfqht9q1ZYHsZYb591GOT8pVKaFCC0z1m  
2kyi++ipy8cUPoDzYmgxVbcdC53+7iLV7aR6spmdl7YogDr+XZAxkSLVPDXj3Ws  
tf8vK3zqEnp1gaAGQrRyeoFDNRSf/bk4uxevpI2ts6iGBzr7lmFIzVsfpA7jkPK  
V2F+j9rlxqbYGD3oNyjg4/hzcDj5v5iWnc82eGYt+arRI5Pm6b7H3vydmfzWKoP  
HvuhbUqqyUwrU6kbBVDDTPM2/04pQxo55MGqz0kUbt+i4KExyaVe+l99czSD/wz  
Y1dV64IpYo90iQlVCCSO+M076F3Cf5loy3jcScRQJnMJ  
-----END CERTIFICATE REQUEST-----  
vManage:~$
```

6. ส่ง cedge01.csr ไปให้ Linux (CA) และทำการ Generate ด้วยคำสั่งนี้

- a. vManage cli

```
scp cedge01.csr root@10.0.0.10:~/  
  
vManage:~$ scp cedge01.csr root@10.0.0.10:~/  
root@10.0.0.10's password:  
cedge01.csr  
vManage:~$
```

- b. Linux (CA)

```
openssl x509 -req -in cedge01.csr -CA SDWAN.pem -CAkey SDWAN.key -CAcreateserial -out  
cedge01.crt -days 2000 -sha256  
  
# openssl x509 -req -in cedge01.csr -CA SDWAN.pem -CAkey SDWAN.key -CAcreateserial  
-out cedge01.crt -days 2000 -sha256  
Certificate request self-signature ok  
subject=C = US, ST = California, L = San Jose, OU = supawit-lab, O = viPtela  
Inc, CN = vedge-CSR-e6bcd73a-88a2-4f28-9075-1b199d09ef86-1.viptela.com, email  
Address = support@viptela.com
```

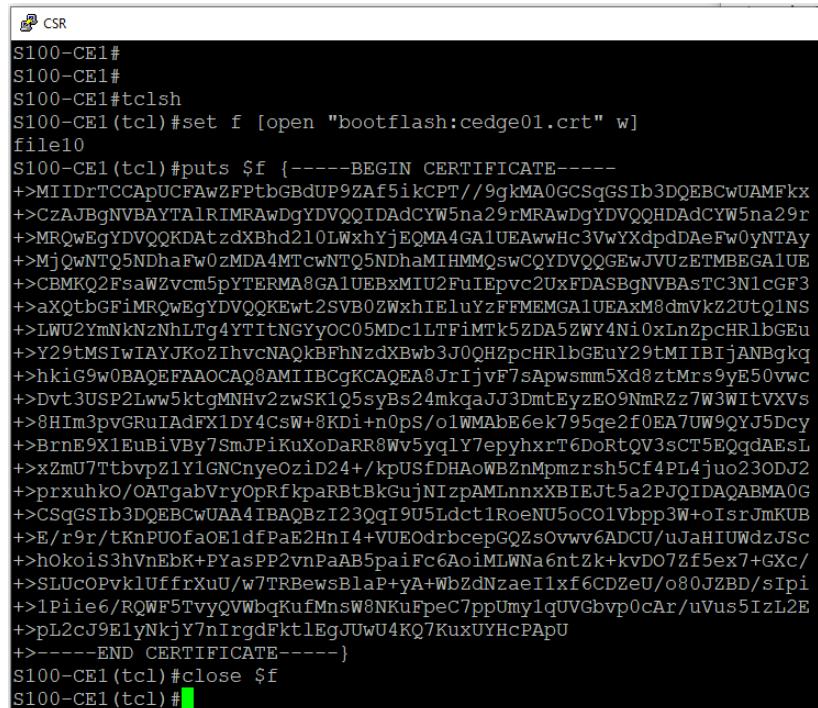
- c. ใช้ vManage ดึง cedge01.crt กลับ

```
scp root@10.0.0.10:cedge01.crt .  
  
vManage:~$ scp root@10.0.0.10:cedge01.crt .  
root@10.0.0.10's password:  
cedge01.crt  
vManage:~$
```

- d. ให้สร้างไฟล์ cedge01.crt ที่ cEdge01 โดยคัดลอกเนื้อหาใน cedge01.crt ที่ vManage ไปยัง cEdge01

```
vManage:~$ cat cedge01.crt
-----BEGIN CERTIFICATE-----
MIIDrTCCApUCFAwZFPtbGBdUP9ZAf5ikCPT//9gkMA0GCSqGSIB3DQEBCwUAMFkx
CzAJBgNVBAYTA1RIMRAwDgYDVQQIDAdCYW5na29rMRAwDgYDVQQHAdCYW5na29r
MRQwEgYDVQQKDAtzdXBhd210LWxhYjEQMA4GA1UEAwHc3VwYXdpdDAeFw0yNTAy
MjQwNTQ5NDhaFw0zMAD4MTcwNTQ5NDhaMIHMMQswCQYDVQQGEwJVUzETMBEGA1UE
CBMKQ2FsaWzvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFDASBjNVBAstC3N1cGF3
aXQtbGFiMRQwEgYDVQQKEwt2SVB0ZWxhIEluYzFFMEMGA1UEAxM8dmVkZ2UtQ1NS
-----END CERTIFICATE-----
```

```
tclsh
set f [open "bootflash: cedge01.crt" w]
puts $f {-----BEGIN CERTIFICATE-----
[ແນ່ນທີ່ key]
-----END CERTIFICATE-----}
close $f
```



```
CSR
S100-CE1#
S100-CE1#
S100-CE1#tclsh
S100-CE1(tcl)#set f [open "bootflash:cedge01.crt" w]
file10
S100-CE1(tcl)#puts $f {-----BEGIN CERTIFICATE-----
+>MIIDrTCCApUCFAwZFPtbGBdUP9ZAf5ikCPT//9gkMA0GCSqGSIB3DQEBCwUAMFkx
+>CzAJBgNVBAYTA1RIMRAwDgYDVQQIDAdCYW5na29rMRAwDgYDVQQHAdCYW5na29r
+>MRQwEgYDVQQKDAtzdXBhd210LWxhYjEQMA4GA1UEAwHc3VwYXdpdDAeFw0yNTAy
+>MjQwNTQ5NDhaFw0zMAD4MTcwNTQ5NDhaMIHMMQswCQYDVQQGEwJVUzETMBEGA1UE
+>CBMKQ2FsaWzvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFDASBjNVBAstC3N1cGF3
+>aXQtbGFiMRQwEgYDVQQKEwt2SVB0ZWxhIEluYzFFMEMGA1UEAxM8dmVkZ2UtQ1NS
+>LWU2YmNkNzNhLTg4YTItNGYyOC05Mdc1LTFiMTk5ZDA5ZWY4Ni0xLnZpcHrlbGEu
+>Y29tMSIwIAYKoZIhvvcNAQbFBhNzdXBwb3J0QHZpcHrlbGEuY29tMIIIBIjANBqkq
+>hkIG9wOBAQEFAAOCQAQ8AMTIBCqKCAQEA8JiJvF7sApwsmm5Xd8ztMrs9yE50vwc
+>Dvt3USP2Lww5ktgMNHv2zWSK1Q5syBs24mkqaJJ3DmtEyzEO9NmRzz7W3WItvxVs
+>8HIm3pvGRuIAdfX1DY4CsW+8KD1+n0ps/o1WMAbE6ek795qe2f0EA7UW9QYJ5Dcy
+>Brne9X1EuBiVby7SmJPiKuXoDaRR8Wv5yqlY7epyhxrt6DoRtQV3sCT5EQqdAESL
+>xZmU7TtbvpZ1YlGNcnyeoziD24+/kpUSfDHaoWBZhMpmzrsh5Cf4PL4juo23ODJ2
+>prxuhkO/OATgabVryOpRfkaRBTkGuNIZpAMLnrxXBIEJt5a2PPQIDAQABMA0G
+>CSqGSIB3DQEBCwUA4IBAQBzI23QqI9U5Ldct1RoeNU5oCO1Vbpp3W+oIsrJmKUB
+>E/r9r/tKnPUOfaoE1dfPaE2HnI4+VUEOdrbcepGQZsovww6ADCu/oJaHTUWdzJSc
+>hokois3hVnEbK+PYasPP2vnPaAB5pafFc6AoimLWNna6ntZk+kvD07zf5ex7+Gxc/
+>SLUcOPvk1UffrXuU/w7TRBewsBlaP+yA+wBZdNzaeIxf6CDzeU/o80JZBD/sIpi
+>1Piie6/RQWF5TvyQVWbqKufMnsW8NKuFpeC7ppUmy1qUVGbvp0cAr/uVus5IzL2E
+>pL2cJ9E1yNkjY7nIrgdFkt1EgJUwU4KQ7KuxUYHcPApU
+>-----END CERTIFICATE-----}
S100-CE1(tcl)#close $f
S100-CE1(tcl)#[
```

ลองตรวจสอบด้วยคำสั่ง dir bootflash: จะต้องมีไฟล์ cedge01.crt

```
dir bootflash:
```

```

total 1098  Feb 24 2025 03:26:58 +00:00  vManage  admin
65025 drwx          4096  Feb 24 2025 05:56:32 +00:00  onep
      21 -rw-           1334  Feb 24 2025 05:56:32 +00:00  SDWAN.pem
      22 -rw-           1220  Feb 24 2025 05:38:55 +00:00  cedge01_csr
      23 -rw-           1334  Feb 24 2025 05:58:57 +00:00  cedge01.crt

7897796608 bytes total (6667984896 bytes free)
S100-CE1#
S100-CE1#
S100-CE1# █

```

7. ลงทะเบียน Certificate ที่ cEdge01

- ใช้คำสั่งนี้ลงทะเบียน

```
request platform software sdwan certificate install bootflash:cedge01.crt
```

- ตรวจสอบด้วย show sdwan certificate serial

```
show sdwan certificate serial
```

```
S100-CE1#show sdwan certificate serial
Chassis number: CSR-e6bcd73a-88a2-4f28-9075-1b199d09ef86 serial number: 0C1914FB
5B1817543FD6407F98A408F4FFFFD824
```

- เปิด Notepad นำ chassis-num , serial number มาแทนที่คำสั่งนี้

```
request vedge add chassis-num [chassis-num] serial-num [serial-number]
```

```
request vedge add chassis-num CSR-e6bcd73a-88a2-4f28-9075-1b199d09ef86
serial-num 0C1914FB5B1817543FD6407F98A408F4FFFFD824
```

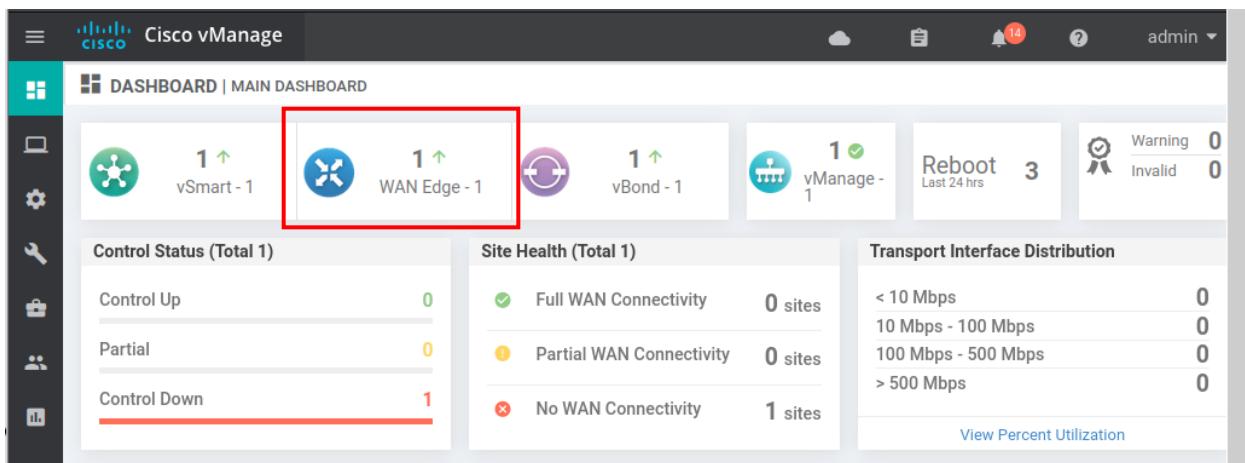
- นำคำสั่งที่ใส่ chassis-num และ serial ที่เตรียมไว้ไปใช้กับ vManage & vBond

```
vBond#
vBond# request vedge add chassis-num CSR-e6bcd73a-88a2-4f28-9075-1b199d09ef86 se
rial-num 0C1914FB5B1817543FD6407F98A408F4FFFFD824
vBond#
vBond# █
vManager
vManager# request vedge add chassis-num CSR-e6bcd73a-88a2-4f28-9075-1b199d09ef86
serial-num 0C1914FB5B1817543FD6407F98A408F4FFFFD824
vManager#
vManager#
vManager#
vManager# █
```

8. หลังจากติดตั้ง Root Certificate เสร็จสิ้นแล้ว กำหนดค่า Tunnel Interfaces : cEdge01

```
config-transaction
!
interface Tunnel 1
no shutdown
ip unnumbered GigabitEthernet1
tunnel source GigabitEthernet1
tunnel mode sdwan
exit
interface Tunnel 2
no shutdown
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
exit
sdwan
interface GigabitEthernet1
tunnel-interface
encapsulation ipsec
color private1
exit
interface GigabitEthernet2
tunnel-interface
encapsulation ipsec
color public-internet
exit
exit
!
commit
end
```

9. รอสักครู่แล้วตรวจสอบที่ vManage GUI



คำสั่งสำหรับตรวจสอบเบื้องต้น

show sdwan control connections

```
s100-CE1#show sdwan control connections
      PEER          SITE      DOMAIN PEER           CONTROLLER          PEER
PEER    PEER PEER      PUB          ID      PRIVATE IP          GROUP          PRIV   PEER
      TYPE     PROT SYSTEM IP      LOCAL COLOR      PROXY STATE UPTIME      ID          PORT  PUBLIC IP
-----+
vsmart  dtls 10.0.0.201      10000      1      10.0.0.200      connect      0          12346 10.0.0.200
          12346 private      0          0      10.10.0.3      up      0:01:23:27  0          12346 10.10.0.3
vbond   dtls -      0      12346 private      1          0      10.10.0.3      connect      0          12346 10.10.0.3
vbond   dtls -      0      12346 public-internet      0          0      10.0.0.100      connect      0          12346 10.0.0.100
vmanage dtls 10.0.0.101      10000      0      10.0.0.100      up      0:00:03:40  0          12346 10.0.0.100
          12346 private      1          0          up      0:00:03:40  0

s100-CE1#
```

cEdge02 (S200-CE1)

ทำตามกระบวนการเดียวกันสำหรับ cEdge02

```
config-transaction
!
hostname S200-CE1
username admin priv 15 secret admin
no ip domain lookup
!
system
system-ip 10.200.10.2
site-id 200
organization-name supawit-lab
vbond 10.10.0.3
exit
!
ip route 0.0.0.0 0.0.0.0 198.51.100.9
ip route 0.0.0.0 0.0.0.0 203.0.113.9
interface GigabitEthernet1
no shutdown
ip address 198.51.100.10 255.255.255.252
interface GigabitEthernet2
no shutdown
ip address 203.0.113.10 255.255.255.252
!
commit
end
```

```

request platform software sdwan root-cert-chain install bootflash:SDWAN.pem

config-transaction
!
interface Tunnel 1
no shutdown
ip unnumbered GigabitEthernet1
tunnel source GigabitEthernet1
tunnel mode sdwan
exit
interface Tunnel 2
no shutdown
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
exit
sdwan
interface GigabitEthernet1
tunnel-interface
encapsulation ipsec
color private1
exit
interface GigabitEthernet2
tunnel-interface
encapsulation ipsec
color public-internet
exit
exit
!
commit
end

```

Summary :

```

tclsh
set f [open "bootflash:SDWAN.pem" w]
puts $f {----BEGIN CERTIFICATE----
[key]
----END CERTIFICATE----}
close $f

request platform software sdwan root-cert-chain install bootflash:SDWAN.pem

request platform software sdwan csr upload bootflash:cedge02_csr

copy to manager (vim cedge02.csr)more bootflash:/cedge02_csr

```

```

send cedge02_csr to kali
scp cedge02.csr root@10.0.0.10:~/

linux
openssl x509 -req -in cedge02.csr -CA SDWAN.pem -CAkey SDWAN.key -CAcreateserial -out cedge02.crt -days 2000 -sha256

ดึงกลับ
scp root@10.0.0.10:cedge02.crt .

cat cedge02.crt

tclsh
set f [open "bootflash:cedge02.crt" w]
puts $f {----BEGIN CERTIFICATE----}
[key]
-----END CERTIFICATE-----
close $f

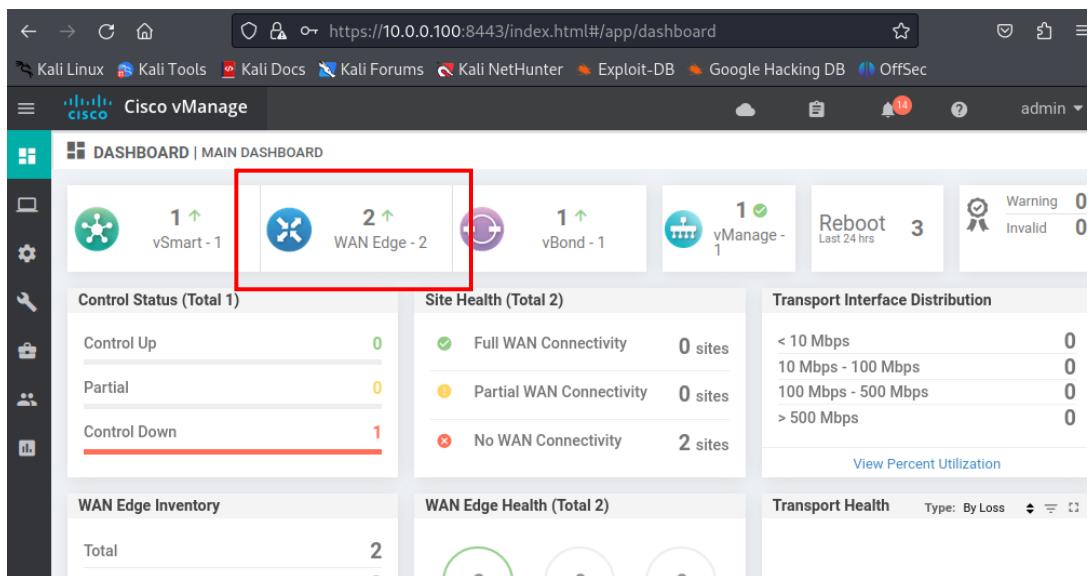
request platform software sdwan certificate install bootflash:cedge02.crt

show sdwan certificate serial

vbond & manage: request vedge add chassis-num CSR-ea80abbc-13cf-4e88-a448-cc4f112e77e1 serial-num
0C1914FB5B1817543FD6407F98A408F4FFFFD825

config tunnel

```



The screenshot shows the Cisco vManage interface under the 'WAN - Edge' tab. The left sidebar has icons for Home, Monitor, Network, Security, Applications, and System. The main area shows a table of devices:

Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BF
vManage	10.0.0.101	vManage	5a795ff3-b3db-4df4-b6f3-eaaabe9...	✓	reachable	10000	--
vSmart	10.0.0.201	vSmart	586b5e10-b635-4134-9055-32e65...	✓	reachable	10000	--
vBond	10.10.0.4	vEdge Cloud (vBo...	6430a83b-1b17-49e0-990e-e8e4f...	✓	reachable	10000	--
S100-CE1	10.100.10.2	CSR1000v	CSR-e6bcd73a-88a2-4f28-9075-1b...	✓	reachable	100	0
S200-CE1	10.200.10.2	CSR1000v	CSR-ea80abbc-13cf-4e88-a448-cc...	✓	reachable	200	0

vEdge (DC1-VE1)

តុលាត្រីយ៉ានី រោចជានា vEdge ទៅ Datacenter ម៉ោងបានក្នុងគ្រប់គ្រងការរំភែកម្មណ៍គ្នាលើក្នុង

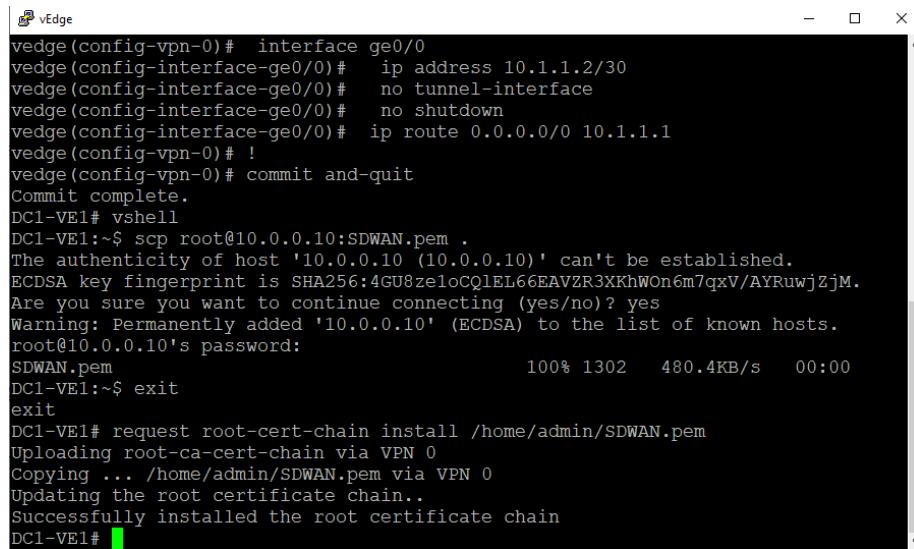
```

conf t
system
host-name DC1-VE1
system-ip 10.1.10.2
site-id 10000
organization-name supawit-lab
vbond 10.10.0.3
!
vpn 0
interface ge0/0
ip address 10.1.1.2/30
no tunnel-interface
no shutdown
ip route 0.0.0.0/0 10.1.1.1
!
commit and-quit

```

```
vshell  
scp root@10.0.0.10:SDWAN.pem .  
exit  
  
request root-cert-chain install /home/admin/SDWAN.pem  
  
conf t  
vpn 0  
interface ge0/0  
tunnel-interface  
encapsulation ipsec  
commit and-quit
```

1.



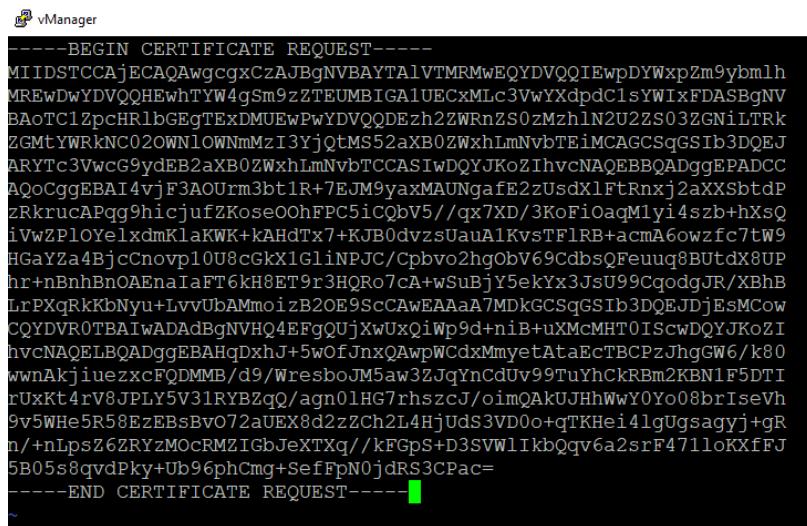
```
vEdge
vedge(config-vpn-0)# interface ge0/0
vedge(config-interface-ge0/0)# ip address 10.1.1.2/30
vedge(config-interface-ge0/0)# no tunnel-interface
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# ip route 0.0.0.0/0 10.1.1.1
vedge(config-vpn-0)#
vedge(config-vpn-0)#
Commit complete.
DC1-VE1# vshell
DC1-VE1:~$ scp root@10.0.0.10:SDWAN.pem .
The authenticity of host '10.0.0.10 (10.0.0.10)' can't be established.
ECDSA key fingerprint is SHA256:4GU8ze1oCQ1EL66EAVZR3XKhWOn6m7qxV/AYRuwjZjM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.10' (ECDSA) to the list of known hosts.
root@10.0.0.10's password:
SDWAN.pem
100% 1302 480.4KB/s 00:00
DC1-VE1:~$ exit
exit
DC1-VE1# request root-cert-chain install /home/admin/SDWAN.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/SDWAN.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
DC1-VE1#
```

2. request csr upload /home/admin/vedge_site10000.csr



```
67:fc:3b:0
DC1-VE1# request csr upload /home/admin/vedge_site10000.csr
Uploading CSR via VPN 0
Enter organization-unit name : supawit-lab
Re-enter organization-unit name : supawit-lab
Organization-unit name differs. Certificate will be deleted. Proceed? [yes,NO] yes
Generating a private/public pair and CSR for this vedge device
Generating CSR for this vedge device .....[DONE]
Copying ... /home/admin/vedge_site10000.csr via VPN 0
CSR upload successful
DC1-VE1#
```

3. copy vedge_site10000.csr from vEdge to vManage (vim)

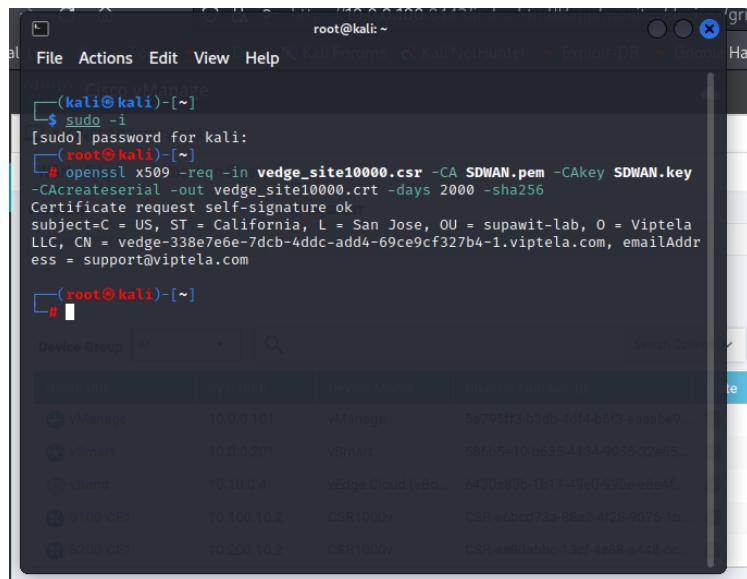


```
-----BEGIN CERTIFICATE REQUEST-----
MIIDSTCCAjECAQAwqcgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MREwDwYDVQQHEwhTYW4gSm9zZTEUMBIGA1UECxMLc3VwYXdpdC1sYWIXFDASBgNV
BAoTC1ZpcHrlbGEgTEXDMUEwPwYDVQDEzh2ZWRnZS0zMzh1N2U2ZS03ZGNiLTrk
ZGmtYWRkNC02OWNl0WNmMzI3yjQtMS52aXB0ZWxhLmNvbTCCASiwdQYJKoZIhv
cNAQEBBQADggEPADCC
AQcggEBAI4vjF3AOUr3bt1R+7EJM9yaxMAUngefE2zUsdX1FtRnxj2aXXSbt
dP
zRkrucAPqg9hicjuFZKoseOohFPC5iCqbV5//qx7XD/3KoFiOaqM1yi4szb+hxsQ
ivWzPloYe1xdmKlaWKW+kAHdTx7+KJB0dvzsUauA1KvsTF1RB+acmA6owzfc7tW9
HGAYza4BjcCnopr10U8cGkX1glnPJC/Cpbvo2hgObV69CdbsqFeuuq8BuTdX8UP
hr+nBnhBnOAEnaIaFT6kH8ET9r3HQRo7cA+wSuBjY5ekYx3JsU99CqodgJR/XBhB
LrpXqRkKbNyv+LvvUbAMmoizB20E9ScCAwEAaA7MDkGCSqGSIB3DQEJDjEsMCow
CQYDVR0TBAlwADAdBgNVHQ4EFgQUjXwUxQiWp9d+niB+uXMcmHT0IScwDQYJKoZI
hvcNAQEELBQADggEBAHqDxhJ+5wOfJnxQAwPWCdxMmyetAtaEcTBCPzJhgGW6/k80
wwnAkjiuezxcFQDMMB/d9/WresboJM5aw3ZJqYnCdUv99TuYhCkRBm2KBN1F5DTI
rUxKt4rV8JPLY5V3LYBZqQ/gn0lHG7rhszcJ/oimQAkUJhhWwYOYo8brIseVh
9v5WHe5R58EzEBsBv072aUEX8d2zzCh2L4HjUds3VD0o+qTKHei4lgUgsagyj+gR
n/+nLpsZ6ZYzMOCRMZIGbJeXTxq//kFGpS+D3SVwlIkbgqv6a2srF471loKxfFJ
5B05s8qvdpky+Ub96phCmg+SeffFpN0jdRS3CPac=
-----END CERTIFICATE REQUEST-----
~
```

4. send vedge_site10000.csr from vmanage to kali

```
scp vedge_site10000.csr root@10.0.0.10:~/  
  
5B05s8qvdpky+Ub96phCmg+SefFpN0jdRS3CPac=  
-----END CERTIFICATE REQUEST-----  
~  
~  
~  
"vedge_site10000.csr" [New File] 20 lines, 1216 characters written  
vManage:~$  
vManage:~$  
vManage:~$  
vManage:~$ scp vedge_site10000.csr root@10.0.0.10:~/  
root@10.0.0.10's password:  
vedge_site10000.csr 100% 1216 853.9KB/s 00:00  
vManage:~$
```

5. Create vedge_site10000.crt



6. ดึงกลับ manage

```
scp root@10.0.0.10:vedge_site10000.crt .  
  
vManage:~$ scp root@10.0.0.10:vedge_site10000.crt .  
root@10.0.0.10's password:  
vedge_site10000.crt 100% 1330 403.  
vManage:~$
```

7. copy vedge_site10000.crt to vEdge

vManager:~\$ cat vedge_site10000.crt

```
-----BEGIN CERTIFICATE-----
MIIDqtCCApECFAwZEPtbGdUDP92Af5ikCPT//9gmMA0GCSqGSIb3DQEBCwUAMFKx
CzA/BgNVBAYTAlRIMRAwgdYVQOHDadCYW5na29rMRQwEgYDVQoKDATzdXbhd210LWxhY
MjQwODEwMzFaPw0zMDA4MTcwODEwMzFaMTHTMsowCQDVQGEWJU1zETMBEGAIUECBMKQ2Fsa
aXQtbGf1LMRQwEgYDVQoKEwLwAxBO2WxhIExMzFBM08GA1UEAxM4dmVkJ22UtMz4
7T2lNmjtN2RjY100ZGBljWk2D0tnj1jZ7l1jZMyN210LEudm1wdGVsY5jb20x
IjAgBgkghk1G9woBCoEW3WchBvcmRdnwdGVsY5jb20x
DQEBAQUMAm1BDwAwQgEKAoIBAQCOL4dwD1K5t27dUfuxtCPemsTAFD1Gnxns1LH
V5Rb0U2y9ml0mXT80ZK7nAD6oPYH17n2sqLHjjc0RTwutgK1ef/6se1w/9ygB
YjmuqNcouM2/oV7E11cg5TMhpCKz1pW1i1vpAB3U8e/i1QH087GrGnSr7bx
UQfmuJncoqM307VvxmmGWAYAp616ddFFHPp9Rp1ryQwvW6NoYmleqvN
W7EBXrtqVAVLXV/FD4/pw24Z2gzbV21GHU+pB/EE/49x0Eo3APsErg120xpGmd
ybPFtQQgHYCUf1wQS6z16Zcmccrv171GwDlqtswdjhPUnqMBAEewDQYJKoZI
hvcNAQELBAGdgBAFA5EZ+*QohywgWEzsrypwScrVfkgsHsgQTwbcJNpRoGVR
DyWR0aFcZKx527tu1FxpVmriglypNSGB9YIK1-LeuBKy31h+oo1/rt44E0L1
9eOUKD9x5hp5gaw2aJc22dMnov762001tRYFt+Qu3c1ojoIvtBUput8Er4on
sKFY2RztFgMsivjgRHtHN65169nkxvLR+m+jRvbY4TMHLep5xuXkIlgruyGMjw6
CkcxoimCBTxLOG5jY0d0RIAvZthDnwNx9AtyR46G6czp/mzAxzIGabz31G74L
M6MaGPcXUJp1gJtDyJXJwdfd/9nrdbg3UNx/RE=
-----END CERTIFICATE-----
```

vManager:~\$

vEdge:~\$

8. request certificate install /home/admin/vedge_site10000.crt

```
DC1-VE1#
DC1-VE1#
DC1-VE1# request certificate install /home/admin/vedge_site10000.crt
Installing certificate via VPN 0
Copying ... /home/admin/vedge_site10000.crt via VPN 0
Successfully installed the certificate
DC1-VE1#
```

9. show certificate serial

10. vmanage & vbond:

request vedge add chassis-num [-] serial-num [-]

```
vBond#
vBond# request vedge add chassis-num 338e7e6e-7dcb-4ddc-add4-69ce9cf327b4 serial
-num 0C1914FB5B1817543FD6407F98A408F4FFFFD826
vBond#
vBond#
```

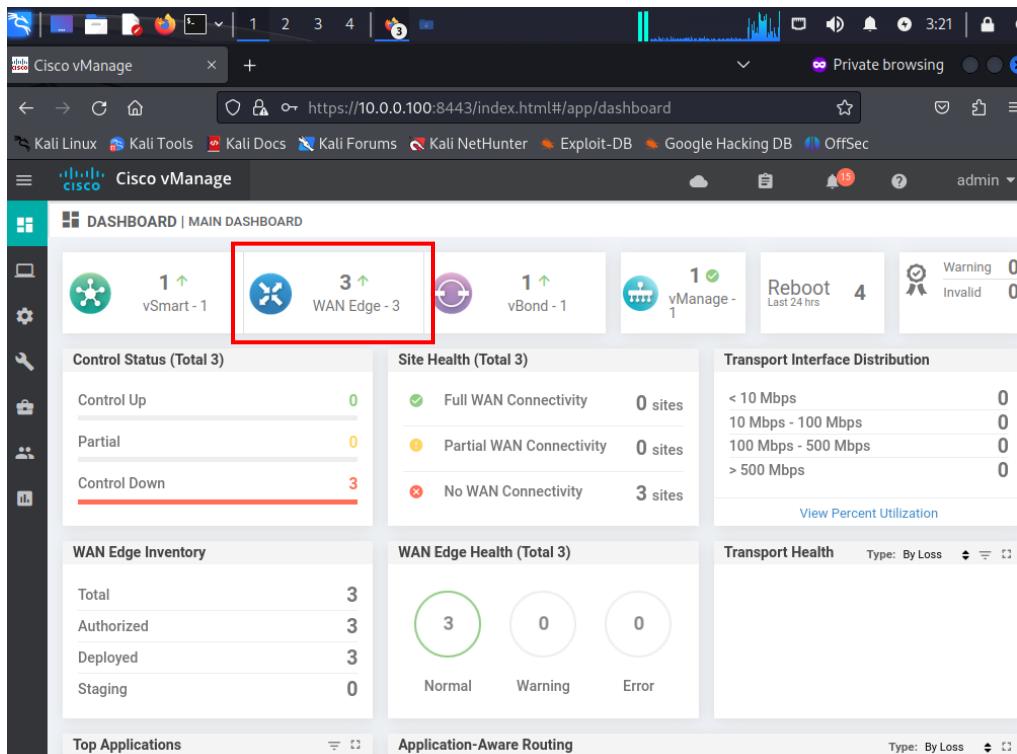


```
vManage# request vedge add chassis-num 338e7e6e-7dcb-4ddc-add4-69ce9cf327b4 serial
-al-num 0C1914FB5B1817543FD6407F98A408F4FFFFD826
vManage#
```

11. Config Tunnel

```
DC1-VE1# conf t
Entering configuration mode terminal
DC1-VE1(config)# vpn 0
DC1-VE1(config-vpn-0)# interface ge0/0
DC1-VE1(config-interface-ge0/0)# tunnel-interface
DC1-VE1(config-tunnel-interface)# encapsulation ipsec
DC1-VE1(config-tunnel-interface)# commit and-quit
Commit complete.
DC1-VE1#
```

12. ตรวจสอบ Dashboard



The screenshot shows the Cisco vManage Main Dashboard. A red box highlights the 'WAN Edge - 3' section, which includes a summary of Control Status (Total 3), Site Health (Total 3), Transport Interface Distribution, WAN Edge Inventory, WAN Edge Health (Total 3), and Transport Health.

Control Status (Total 3)	Site Health (Total 3)	Transport Interface Distribution
Control Up: 0	Full WAN Connectivity: 0 sites	< 10 Mbps: 0
Partial: 0	Partial WAN Connectivity: 0 sites	10 Mbps - 100 Mbps: 0
Control Down: 3	No WAN Connectivity: 3 sites	100 Mbps - 500 Mbps: 0
		> 500 Mbps: 0

WAN Edge Inventory	WAN Edge Health (Total 3)	Transport Health
Total: 3	Normal: 3	Type: By Loss
Authorized: 3	Warning: 0	
Deployed: 3	Error: 0	
Staging: 0		

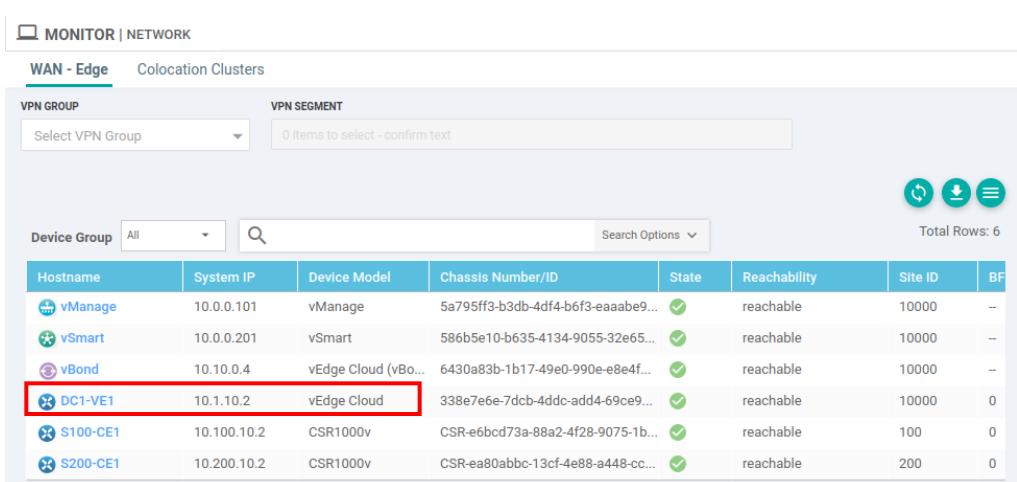
WAN Edge Inventory:

- Total: 3
- Authorized: 3
- Deployed: 3
- Staging: 0

WAN Edge Health (Total 3):

- Normal: 3
- Warning: 0
- Error: 0

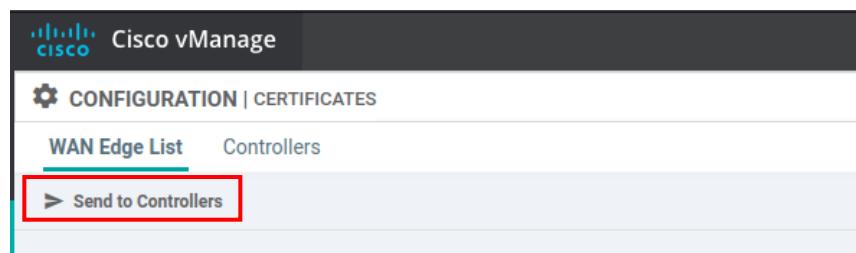
Transport Health: Type: By Loss



The screenshot shows the Cisco vManage MONITOR | NETWORK WAN - Edge tab. A red box highlights the 'DC1-VE1' entry in the Device Group table. The table lists various devices and their status.

Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BF
vManage	10.0.0.101	vManage	5a795ff3-b3db-4df4-b6f3-eaaabe9...	✓	reachable	10000	—
vSmart	10.0.0.201	vSmart	586b5e10-b635-4134-9055-32e65...	✓	reachable	10000	—
vBond	10.10.0.4	vEdge Cloud (vBo...)	6430a83b-1b17-49e0-990e-e8e4f...	✓	reachable	10000	—
DC1-VE1	10.1.10.2	vEdge Cloud	338e7e6e-7dc8-4ddc-add4-69ce9...	✓	reachable	10000	0
S100-CE1	10.100.10.2	CSR1000v	CSR-e6bcd73a-88a2-4f28-9075-1b...	✓	reachable	100	0
S200-CE1	10.200.10.2	CSR1000v	CSR-ea80abbc-13cf-4e88-a448-cc...	✓	reachable	200	0

13. Configuration > Certificates > Send to Controllers



The screenshot shows the Cisco vManage CONFIGURATION | CERTIFICATES WAN Edge List tab. A red box highlights the 'Send to Controllers' button.

DC1-SW2 & S100-SW1 & S200-SW1

```

host S100-SW1 #แก้ไขชื่อ กับหมายเลข IP ให้ตรงตาม Topo
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
vlan 10
vlan 20
vlan 30
!
interface Vlan10
ip address 10.100.10.254 255.255.255.0
no sh
!
interface Vlan20
ip address 10.100.20.254 255.255.255.0
no sh
!
interface Vlan30
ip address 10.100.30.254 255.255.255.0
no sh
!
ip route 0.0.0.0 0.0.0.0 10.100.10.1
ip route 0.0.0.0 0.0.0.0 10.100.20.1 5
ip route 0.0.0.0 0.0.0.0 10.100.30.1 10
!
end

```

Interface IPs:

- DC1-FW1:
 - g0/0 > 10.1.0.1 /30
 - g0/1 > 10.10.0.1 /24
 - g0/2 > 198.51.100.2 /30
 - g0/3 > 203.0.113.2 /30
- DC1-SW1:
 - VLAN 1 > 10.0.0.1 /24
 - VLAN 2 > 10.1.0.1 /30

- VLAN 10 > 10.1.1.1 /30
- DC1-SW2:
 - VLAN 10 > 10.1.10.254 /24
 - VLAN 20 > 10.1.20.254 /24
 - VLAN 30 > 10.1.30.254 /24
- DC1-VE1:
 - ge0/0 > 10.1.1.2 /30
 - ge0/1.10 > 10.1.10.1 /24
 - ge0/1.20 > 10.1.20.1 /24
 - ge0/1.30 > 10.1.30.1 /24
- S100-CE1:
 - g1 > 198.51.100.6 /30
 - g2 > 203.0.113.6 /30
 - g3.10 > 10.100.10.1 /24
 - g3.20 > 10.100.20.1 /24
 - g3.30 > 10.100.30.1 /24
- S100-SW1:
 - VLAN 10 > 10.100.10.254 /24
 - VLAN 20 > 10.100.20.254 /24
 - VLAN 30 > 10.100.30.254 /24
- S200-CE1:
 - g1 > 198.51.100.10 /30
 - g2 > 203.0.113.10 /30
 - g3.10 > 10.200.10.1 /24
 - g3.20 > 10.200.20.1 /24
 - g3.30 > 10.200.30.1 /24
- S200-SW1:
 - VLAN 10 > 10.200.10.254 /24
 - VLAN 20 > 10.200.20.254 /24
 - VLAN 30 > 10.200.30.254 /24
- SP1:
 - g0/0 > 198.51.100.1 /30
 - g0/1 > 198.51.100.5 /30
 - g0/2 > 198.51.100.9 /30
 - g0/3 > 192.0.2.1 /30
- SP2:
 - g0/0 > 203.0.113.1 /30
 - g0/1 > 203.0.113.5 /30
 - g0/2 > 203.0.113.9 /30
 - g0/3 > 192.0.2.2 /30