# ةيامح رادج مادختساب نمآلا لوصولا نيوكت Sophos XG

# تايوتحملا

<u>ةمدقملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>قيساسأ تامولعم</u> <u>نى وكتلا</u> <u>نمآلاا لوصولا يلع قفناا نيوكت</u> <u>ق ف ن ا ت ان اي ب</u> <u>Sophos ىلع قفنلا نېوكت</u> <u>IPsec فيرعت فالم نيوكت</u> <u>عقوم ىلا عقوم نم VPN ةكبش نىوكت</u> <u>قفنلا ةمجاو نيوكت</u> <u>تاباوبلا نيوكت</u> SD-WAN راس م نېېوكټ <u>صاخلا قيبطتالا نيوكت</u> <u>لوصولا چەن نېوكت</u> <u>قحصالا نم ققحتاا</u> <u>VPN-ار</u> <u>ىساسألالىمعلا ZTNA</u> <u>ضرعتسملا الانتسملا على الانتسمل ZTNA</u> <u>ةلص تاذ تامولعم</u>

# ەمدقملا

.Sophos XG ةيامح رادج مادختساب نمآلا لوصولا نيوكت ةيفيك دنتسملا اذه حضوي

# ةيساسألا تابلطتملا

- <u>مدختسملا ريفوت نيوكت</u> •
- <u>ZTNA SSO ةقداصم نيوكت</u>
- <u>دعب نع لوصول VPN دلإ نمآلا لوصولا نيوكت</u> •

# تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- Sophos XG ةيامح رادج •
- نمآلا لوصولا

- Cisco Secure Client VPN
- Cisco Secure Client ZTNA
- اياوز نودب انتز •

ةمدختسملا تانوكملا

ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- Sophos XG ةيامح رادج •
- نمآلا لُوصُولاً •
- Cisco Secure Client VPN
- Cisco Secure Client ZTNA

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

# ةيساسأ تامولعم

# CISCO Secure Access SOPHOS

Sophos - نمآلا لوصولا

، ،ەريفوتو ةصاخلا تاقيبطتلا ىلإ لوصولا ةيامح نامضل Secure Access ةزيم Cisco تممص ةكبشلا نم لاصتالا نمضي ەنأ امك .ءاوس دح ىلع ةكبشلا ىلع مئاقو يلحم ساسأ ىلع اهعيمج فدهت ،ةددعتم ةينمأ تاقبطو بيلاسأ قيبطت لالخ نم كلذ ققحتيو .تنرتنإلا ىلإ قباحسلا ربع اهيلإ لوصولا دنع تامولعملا ىلع ظافحلا ىل

# نيوكتلا

# نمآلا لوصولا ىلع قفنلا نيوكت

# ب ةصاخلا ةرادإلا ةحول ىلإ لقتنا <u>Secure Access</u>.



ةيسيئرلا ةحفصلا - نمآلا لوصولا

• اقوف رقن Connect > Network Connections.

Overview	Overview
💉 Connect	The Overview dashboard displays Essentials
Resources	Network Connections Connect data centers, tunnels, resource connectors
Secure Secure	Users and Groups Provision and manage users and
Monitor	groups for use in access rules
2o Admin	Manage traffic steering from endpoints to Secure Access
ةكبشلا تالاصتا - نمآلا لوصولا	

• تحت Network Tunnel Groups ا تحت + Add.

vork Tunnel Groups 21	total						
onnected ()	1 Warning 🔺	O Connected Ø					
work Tunnel Group twork tunnel group provid ibility. Connect tunnels to access to the Internet an Search	DS des a framework for establishing tunnel the hubs within a network tunnel group d private resources. Help C Region	redundancy and high p to securely control Status V 2 Tunnel Grou	DS				
			-				
etwork Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels	
etwork Tunnel Group	Status  O Disconnected	Region Europe (Germany)	Primary Hub Data Center	Primary Tunnels 0	Secondary Hub Data Center	Secondary Tunnels	
etwork Tunnel Group OME AD	Status	Region Europe (Germany) Europe (Germany)	Primary Hub Data Center sse-euc-1-1-0 sse-euc-1-1-0	Primary Tunnels 0 1	Secondary Hub Data Center sse-euc-1-1-1 sse-euc-1-1-1	Secondary Tunnels 0 0	

ةكبشلا قفن تاعومجم - نمآلا لوصولا

- Device Type. نيوكتلا Device Type.
- رقنا. Next

# **General Settings**

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

# **Tunnel Group Name**

SophosFirewall	$\otimes$
Region	
Europe (Germany)	~ )
Device Type	
Other	~

# Cancel

ةماعلا تادادعإلاا - قافنألاا تاعومجم - نمآلا لوصولا

Next



ةيامحلا رادج عقوم ىلإ ةقطنم برقأ رتخأ :**نَظح**الم.

- Passphrase. و Tunnel ID Format نيوكتب مق
- Next.رقنا •

# **Tunnel ID and Passphrase**

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format		
Email IP Address		
Tunnel ID		
csasophos (a) @ <org><hub>.sse.cisco.com</hub></org>		
Passphrase		
•••••	Show	$\otimes$
The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case let number, and cannot include any special characters.	tter, one	)

#### **Confirm Passphrase**

••••••	Show $\otimes$
Cancel	Back

رورملا ةرابعو قفنلا فرعم - قافنألا تاعومجم - نمآلا لوصولا

• قكرح ريرمت ديرتو ةكبشلا ىلع اەنيوكتب تمق يتلا ةفيضملا تائيبلا وأ IP نيوانع تاقاطن نيوكتب مق نمآلا لوصولا لالخ نم رورملا.

• رقنا. Save

# **Routing option**

#### Static routing

Use this option to manually add IP address ranges for this tunnel group.

#### **IP Address Ranges**

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

	128.66.0.0/16, 192.0.2.0/24	Add	
)	192.168.0.0/24 × 192.168.10.0/24 ×		
	Use this option when you have a BGP peer for your on-premise router.		
Can	cel		Back Save
صولا	ەيجوتال تارايخ - قافنألا تاعومجم - نمآلا لو		

ةيلات القوف رقنلا دعب Save ،قيلات المولعمل التامول من التن تعليم المرع لوح المرع لوح Save تامول عمل التام دعب Sophos. قڧنلا تانايب

# Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	csasophos@	-sse.cisco.com	a
Primary Data Center IP Address:	18.156.145.74 🗇		
Secondary Tunnel ID:	csasophos@	-sse.cisco.com	đ
Secondary Data Center IP Address:	3.120.45.23 🗇		
Passphrase:	đ		



نيوكتلا فانئتسإ - قافنألا تاعومجم - نمآلا لوصولا

Sophos ىلع قڧنلا نيوكت

IPsec فيرعت فلم نيوكت

.كب صاخلا Sophos XG ةيامح رادج ىلإ لقتنا ،IPsec فيرعت فلم نيوكتل

اذەل ەباشم ءيش ىلع لصحت:



ةرادإلا ةحول - Sophos

- Profiles ىلإ لقتنا
- IPsec Profiles قوف رقنا Add



IPsec فيرعت تافلم - Sophos

# نيوكتلا General Settings تحت:

- Name: نم نمآلا لوصولا جەنل عجرم مسا Cisco
- Key Exchange: IKEv2
- Authentication Mode: يسيئرلاا عضولاا
- Key Negotiation Tries:0
- Re-Key connection: رايخلا ددح

Name	Description	
CSA	Description	
Key exchange	Key negotiation tries	Re-key connection
Authentication mode	Set 0 for unlimited number of negotiation tries	<ul> <li>Pass data in compressed format</li> <li>SHA2 with 96-bit truncation</li> </ul>

ةماع تادادعإ - IPsec تافيصوت - Sophos

# :نيوكتلا 1 Phase تحت

- Key Life:28800
- DH group(key group): و 19 و 19 ديدحت
- Encryption: AES256
- Authentication: SHA2 256
- Re-key margin: 360 (ايضارتفالا)
- Randomize re-keying margin by: 50 (ايضارتفا)

Phase 1

Key life		Re-key margin		Randomize re-keying margin by	
28800	•	360	•	50	•
	Seconds		Seconds		%
DH group (key group)					
2 selected	0 -				
Encryption		Authentication			
AES256	<b>o</b> ~	SHA2 256	<b>o</b> ~		

1 ةلحرملا - IPsec فيرعت تافلم - Sophos

# :نيوكتلا 2 Phase تحت

- PFS group (DH group): ىلوألا ةلحرملا سفن
- Key life:3600
- Encryption: AES 256
- Authentication: SHA2 256

# Phase 2

PFS group (DH group)		Key life	
Same as phase-I	⊘∽	3600	0
			Seconds
ncryption		Authentication	

2 ةلحرملا - IPsec فيرعت تافلم - Sophos

# نيوكتلا Dead Peer Detection تحت:

- Dead Peer Detection: رايخلا ددح
- Check peer after every:10
- Wait for response up to: 120 (إيضارتفالا)
- When peer unreachable: (يضارتفالا) ءدبلا ةداع

# BEFORE

Check peer after every	Seconds	Wait for response up to	Seconds	When peer unreachable Re-initiate	© ~
AFTER					
AFTER  Dead Peer Detection Check peer after every		Wait for response up to		When peer unreachable	

تيملا ريظنلا فاشتكا - IPsec فيرعت تافلم - Sophos

طغضا كلد دعب Save and proceed with the next step, Configure Site-to-site VPN.

عقوم ىلإ عقوم نم VPN ةكبش نيوكت

Reports Zero-day protection Diagnostics	Show additional properties	Add	Delete	Wizard
PROTECT Rules and policies	□ Name □ ▲ Group name □ Profile □ Connection type	Status	Connection 7	Manage
Intrusion prevention Web Applications	No records found			
Wireless Email Web server				
Advanced protection	Failover group			
CONFIGURE Remote access VPN				
Site-to-site VPN Network			Add	Delete

Add. قوف رقنا مث Site-to-site VPN قوف رقنا ،(VPN) ةيرهاظلا ةصاخلا ةكبشلا نيوكت ءدبل

عقوم ىلإ عقوم نم VPN ةكبش - Sophos

# نيوكتلا General Settings تحت:

- Name: نم نمآلا لوصول ال IPsec جەنل عجرم مسا Cisco
- IP version: IPv4
- Connection type: قەخال قەجاو
- Gateway type: لاصتالا عدب



.عقوم ىل| عقوم نم VPN ةكبش نيوكت ىل| يەتنت نأ دعب ايئاقلت VPN ةكبش رايخلا نكمي Active on save :مطّحالم

General settings			
Name SecureAccesS	IP version IPv4 O IPv6 O Dual		<ul><li>Activate on save</li><li>Create firewall rule</li></ul>
Description This is the IPsec Policy for Sophos	Connection type Tunnel interface	<b>o</b> ~	
	Gateway type Initiate the connection	<b>o</b> ~	

ةماع تادادعإ - عقوم ىلإ عقوم نم VPN ةكبش - Sophos



.XFRM مساب Sophos XG ةيامح رادجل ةيضارتفا قفن ةهجاو ءاشنإب ةيرايتخالا قفنلا ةهجاو موقت :مَطْحالم

نيوكتلا Encryption تحت:

- Profile ،ةوطخلا ىلع مىاشنإب موقت يذلا فيرعتالا فالم .Configure IPsec Profile
- Authentication type: اقبسم كرتشملاحات
- Preshared key: ،ةوطخلا ىل منيوكتب موقت يذلا حاتفملا <u>Configure the Tunnel on Secure Access</u>
- Repeat preshared key: Preshared key

# Encryption Profile Authentication type CSA Image: CSA Preshared key Image: CSA Preshared key Image: CSA Repeat preshared key Image: CSA Repeat preshared key Image: CSA CSA Image: CSA

ريفشتالا - عقوم يال عقوم نم (VPN) ةيرهاظالا قصاخالا قكبشالا - Sophos

.عجرمك لودجلا اذه مدختسأ ، Local Gateway Remote Gateway نيوكتلا تارايخ Gateway Settings تحت

ةيلحملا ةباوبلا	ةديعبلا ةباوبلا
عامتسالا ةەجاو كيدل تنرتنإلا-WAN ةكبش ةەجاو	ةباوبلا ناونع ،ةوطخلا بجومب ەؤاشنإ مت يذلا ماعلا IP ، <u>Data</u>
يلحملا فرعملا عون ينورتكلإلا ديربلا	ديعبلا فرعملا عون

	IP ناونع
يلحم فرعم	ديعب فرعم
تحت ەۋاشنإ مت يذلا ينورتكلإلا ديربلا	،ةوطخلا بجومب ەؤاشنإ مت يذلا ماعلا IP ،
،ةوطخلا	<u>Data</u>
ةيلحملا ةيعرفلا ةكبشلا	ةديعبلا ةيعرفلا ةكبشلا
يأ	يأ

Sateway settings			
Local gateway		Remote gateway	
Listening interface		Gateway address	
PortB - 192.168.0.33	•	18.156.145.74	0
Local ID type		Remote ID type	
Email	⊘ ~	IP address	<b>o</b> ~
Local ID		Remote ID	
csasophos@ -sse.cisco.com	0	18.156.145.74	0
Local subnet		Remote subnet	
Any	0	Any	0
Add new item		Add new item	

ةباوبلا - عقوم ىل عقوم نم (VPN) ةيره اظلا قصاخلا قكبشلا تادادع - Sophos

# ەۋاشنإ مت قەنلا نأ ىرت نأ كنكميوSave ،رقنا كلذ دعب.

Psec co	onnections							
Show	v additional properties					Add	Delete	Wizard
		0	Deefle 🖂	Occupation to an a	Status			Manage
	Name V	Group name 1	Profile V	Connection type 1	Active 🕎	Connecti	on 7	Manage
	SecureAccesS	-	CSA	Tunnel interface	•	• 1		💉 👁 🗊



اذإ ،ةلاحلا Connection نم ققحتلا كنكمي ،ةريخألا ةروصلا ىلع حيحص لكشب قفنلا نيكمت نم ققحتلل :<del>تظح</del>لام لصتم ريغ قفنلا ارضخأ نكي مل اذإ لصتم قفنلا نإف ،ارضخأ ناك.

Current Activities > IPsec Connections. كل لقت القن عاشن إمت اذا امم ققحت ل

MONITOR & ANALYZE Control center Current activities Reports Zero-day protection Diagnostics

Sophos - ليلحتاو ةبقارما - IPsec

	Live users	Live conn	ections	Live connections IPv6	IPsec cor	nnections	Remote users	
No t	unnel established	to Secure Acces	s					
, 🗆	Name 🍸	Local server 🖓	Local subnet 🕤	7 Username ∏	Remote server/host	Remo	ote subnet 🛛	Manage
No rec	cords found							
Tunr	nel established to	Secure Access		0				
	Name 🖓	Local server 7	Local subnet 🗧	7 Username 7	Remote server/host	Remote	subnet 🕎	Manage
	SecureAccesS-1	192.168.0.33	0.0.0/0		18.156.145.74	0.0.0.0/	0	s <sup>56</sup>

دعبو لبق IPsec - ليلحتلاو ةبقارملا - IPsec

، موطخلا لصاون نأ نكمي ،كلذ دعبو، Configure Tunnel Interface Gateway.

#### قڧنلا ةەجاو نيوكت

مادختساب ةيرهاظلا قفنلا قەجاو ريرحتل WANاەصحفو VPN ةكبش ىلع اەنيوكت مت يتلا Network قەجاولا ىلإ لىقتنا مسالا xfrm.

.ةەجاولا xfrm ىلع رقنا

Wireless	Physical
Email Web server Advanced protection	WAN WAN Physical
CONFIGURE Remote access VPN Site-to-site VPN	xfrm1 Unnel VPN
Network Routing Authentication System services	Eth PortC Unbound Physical

قەنلا تەجاو - تەكبشلا - Sophos

• مادختسإ كنكمي ،لـاثملا ليبس ىلع ،كتكبش يف ەيجوتلل لباقلا ريغ IP مادختساب ةەجاولا نيوكتب مق 169.254.x.x/30 مدختسن ەلـثمن يذلا لـاثملا يفو ،ةداع ەيجوتلل قلباق ريغ قحاسم يف IP وەو 169.254.x.x/30

General settings			
Name *	xfrm1		
Hardware	xfrml		
IPsec connection	SecureAccesS		
Network zone	VPN		
IPv4/netmask *	169.254.0.1	/30 (255.255.255.252)	~

نيوكتلا - قفنلا ةهجاو - ةكبشلا - Sophos

## تاباوبلا نيوكت

(xfrm) ةيرەاظلا ةەجاولا ةرابع نيوكتل

- القتنا Routing > Gateways
- Add رقنا •

Diagnostics	SD-WAN rou	tes SD-WAN	profiles	Gateways	Static routes	BGP	OSPF	0SPFv3	Information	Upstream proxy	
PROTECT Rules and policies Intrusion prevention	IPv4 gat	teway									
Web Applications Wireless									Ad	d Delete	e
Email Web server		Name 🍸		IP addres	is 🖓 🛛 I	nterface 🖓	Health	check 🖓	Status 🍸	Manage	
Advanced protection		DHCP Port	<u>B GW</u>	192.168	.0.1 \	WAN	On		•		
Remote access VPN Site-to-site VPN Network											

تاباوبلا - ەيجوتلا - Sophos

# نيوكتلا Gateway host تحت:

- Name: قكبشل اهؤاشنإ مت يتلا قيرهاظل قهجاول عل ريشي مسا VPN
- Gateway IP: ان ال 169.254.0.2، ان مق يذل 169.254.0.1/30 تاترتن (IP) تن رتن (IP) تاب ال وكوتورب وه اذه موطخل اتحت لعفل اب من ي عتب Configure Tunnel Interface
- Interface: ةكبشل ةيرهاظلا مجاولا VPN
- Zone: (يضارتفالا)) الب

# Gateway host Name \* CSA\_GW Gateway IP 169.254.0.2 Interface xfrm1-169.254.0.1 Zone None

ةباوبلا فيضم - تاباوبلا - هيجوتلا - Sophos - هجوتلا -

- ققحتالا ليطعت Health check تحت
- رقنا Save

# Health check

# Health check



ةحصلا نم ققحتلا - تاباوبلا - هيجوتلا - موجوتلا

# نيوكتلا ظفح دعب ةباوبلا ةلاح ةظحالم كنكمي:

IP	v4 ga	teway					
						Add	Delete
		Name 🍸	IP address 🖓	Interface 🖓	Health check 🛛	Status 🖓	Manage
		CSA GW	169.254.0.2	xfrml	Off	•	1 🔿 🕅
		DHCP PortB GW	192.168.0.1	WAN	On	•	

ةلاحلا - تاباوبلا - ميجوتلا - Sophos

# SD-WAN راسم نيوكت

نمآلا لوصولا ىل رورملا ةكرح هيجوت ةداعإب كل حمسي يذلا راسملا ءاشنإ كمزلي ،نيوكتلا ةيلمع ءاهنإل.

#### القتنا Routing > SD-WAN routes.

Add قوف رقنا

Diagnostics	*	SD-V	VAN routes	SD-WAN profiles	Gateways	Static routes	BGP	OSPF	OSF
PROTECT Rules and policies Intrusion prevention Web Applications Wireless Email		0	Current prec Policy route	edence for routing. St also applies to system	atic route, SD-WAN ro -generated and reply	oute, VPN route. • traffic. To learn how f	to change the configu	ration, go to the <mark>onlin</mark> e	∍ help.
Web server Advanced protection CONFIGURE Remote access VPN Site-to-site VPN Network		IPv4	SD-WAN I	route	📕 Watch: Ho	w to use SD-WAN ro	utes		Add
Authentication کبش - Sophos قرط	Jö W	ے ہملا AN	 لا نع ةفرع	جماربلا قيره		Destination	o 🗁	Application	in 🖂

#### نيوكتلا Traffic Selector تحت:

• Incoming interface: وأ RA-VPN نم نولصي نيذلا نيمدختسملا وأ رورملا ةكرح لاسرا ديرت ثيح نم ةمجاولا ددح RA-VPN و وا ClientLess-ZTNA

- DSCP marking: لاه ىلع ءيش ال
- Source networks: قفنلا ددح source networks: قفنل اربع مەيجوت ديرت يذل اناونعل
- Destination networks: ةەجو ديدحت كنكمي وأ يأ
- Services: تامدخلا ديدحت كنكمي وأ يأ
- Application object: نئاكلا نيوكت مت اذإ قيبطت
- نمآلا لوصولا ىل رورملا ةكرح هيجوتل نيمدختسملا نم ةنيعم ةعومجم ةفاض إيف بغرت تنك اذا User or groups: نمآلا لوصول اىل

# Traffic selector

Incoming interface		DSCP marking			
LAN-192.168.0.203	•	Select DSCP marking	•		
Source networks		Destination networks		Services	
Any	0	Any	0	Any	0
Add new item		Add new item			Add new item
Application object		User or groups			
Any	0	Any	0		
Add new item		Add new item			

رورملا ةكرح ددحم - SD-WAN تاراسم - SOPHOS

#### تحت Link selection settings تحت:

- Primary and Backup gateways: رايخلا ددح
- Primary gateway: ،ةوطخلا نمض ةنوكملا ةباوبلا ديدحت، <u>Configure the Gateways</u>
- قوف رقنا Save

Link selection settings		
O Select SD-WAN profile 🕧 O Primary and	Backup gateways	
Primary gateway	Backup gateway	
CSA_GW	None	
Route only through specified gateways ()		
Save Cancel		

، دوطخلاب تعامنا دعب Sophos XG، موطخلاب تعامنا عامن العنا عامن العامن العامن العامن العامن العامن العامي العامي

صاخلا قيبطتلا نيوكت

ل<u>وؤس ملاا لخدم</u> ىلإ لوخدلا ليجستب مق ،صاخلا قيبطتلا يلإ لوصولا نيوكتل.

• القتنا Resources > Private Resources

Overview	<b>Private Resources</b>
Connect	Private Resources are applications, r resource using zero-trust access. He Private Resources Private F
Resources	Sources and destinations
Secure	Private Resources Define internal applications and other resources for use in access
Monitor	rules Registered Networks
Lo Admin	Point your networks to our servers
Workflows	to use as sources in access rules
	Internet and SaaS Resources Define destinations for internet access rules <b>Roaming Devices</b> Mac and Windows

ةصاخلا دراوملا - نمآلا لوصولا

Add + قوف رقنا

Private Resources Private Resource Groups							
Private Resourc	ces					◯ Last 24 Hours ∨	
Q Search by resou	Irce name Privat	te Resource Group	✓ Connection	Method V 4 Private Res	ources	+ Add	
Private Resource		Private Resource Group	Connection Method	Accessed by	Rules	Total Requests	

<sup>2</sup> ةصاخلا دراوملا - نمآلا لوصولا

• نيوكت General تحت Private Resource Name

# General

# **Private Resource Name**

SplunkSophos

**Description** (optional)

ماع - ةصاخلا دراوملا - نمآلا لوصولا

تحت Communication with Secure Access Cloud تحت

• Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR): هيل| لوصول اديرت يذل ادرومل اددح



ةوطخلا يف ايلخاد هيلإ لوصولل لباقلا ناونعلا نييعت مت دق هنأ ركذت :<del>تظح</del>الم، <u>Configure the Tunnel on Secure</u> <u>Access</u>.

- Protocol: دروملا اذه ىل لوصول له مدختست يذل لوكوتوربلا ديدجت
- Port / Ranges : قيبطتلا علاا ديدحت عن الجاتحت عن الفانمل الميدحت Port / Ranges •

Communication with Secure Access Cloud				
Specify one or more addresses that will be used for communication between the	his resource and Secure A	Access. Secure Access wil	I route traffic to this address. Help 🗗	
Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR) ③ 192.168.0.40	Protocol TCP - (HTTP/HTTPS	Port / Ranges	+ Protocol & Port	
+ IP Address or FQDN Use internal DNS server to resolve the domain				~

Secure Access - مادختساب تالاصتالا - قصاخلا دراوملا - Secure Access مادختساب

نمضو Endpoint Connection Methods الما عيمج نيوكت كنكمي ،ةدحولا مذه Endpoint Connection Methods نمضو اكتئيبل اممادختسإ ديرت يتلا قرطلا رتخاو ،"نمآلا لوصولاا":

- Zero-trust connections: لوصو نيكمتل عبرملا ددح ZTNA.
  - Client-based connection:: ليمعلاب قصاخلا انتز قدعاقب حامسلل رزلا نيكمت
    - Remotely Reachable Address: م) اخل IP نيوكت
    - Browser-based connection:: ضرعتسملا ا ىل قدنتسمل ZTNA ل حامسلل رزلا نيكمت
      - vtna.sse.cisco.com لاجملاع منارتق الاب ممادخت سال مسا قفاض ztna.sse.cisco.com
        - ضرعتسمل الالخ نم ميل الوصول لوكوتوربك HTTPS وأ HTTP رتخاً .
    - VPN connections: لوصو نيكمتل عبرملا ددح RA-VPN.
- Save رقنا

Zero-trust connections	
Allow endpoints to connect to this resource from	n outside your network without requiring a VPN connection. <b>Help</b> 🗗
Client-based connection Allow connections from endpoints that have the	Secure Client installed. Enable this option for maximum control over
Remotely Reachable Address (FQDN, Wildcard	I FQDN, IP Address) ①
192.168.0.40	
+ FQDN or IP Address	
Allow browser-based connections from endpoin endpoint security checks are possible. Public URL for this resource ①	ts that do not have the Secure Client installed. Enable this option wh
https:// splunksophos	-8195126.ztna.sse.cisco.com
Protocol     Server Name Indication (SNI)       HTTP        Validate Application Certificate ③	(optional) ①
VPN connections	

Allow endpoints to connect to this resource when connected to the network using VPN.

Save	Cancel

Secure Access - مادختساب تالاصتالا - قصاخلا دراوملا - Secure Access Cloud 2

# ةجيتنلا يه هذه نوكت ،نيوكتلا لامتكا دعب:

Private Resource	÷	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests	
SplunkSophos		-	VPN Browser-based ZTNA Client-based ZTNA	1	2	16	

، configure the Access Policy. ،ةوطخلا ةعباتم كنكمي نآلا

لوصولا جەن نيوكت

ىل| لوصولا جەن نيوكتل Secure > Access Policy.

Secure	Policy
Monitor	Access Policy Create rules to control and secure access to private and internet
Admin	destinations

لوصولا ةسايس - نمآلا لوصولا

• رقنا Add Rule > Private Access

# Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

# Internet Access

Control and secure access to public destinations from within your network and from managed devices

صاخلا لوصولا - لوصولا ةسايس - نمآلا لوصولا

ةقداصملل ةددعتم قرط ربع لوصولا ريفوتل ةيلاتلا تارايخلا نيوكتب مق:

1. Specify Access

ĉ

- حامس:Action
  - Rule name: كب ةصاخلا لوصول أقدعاقل مسا ديدحت
  - From: ىل لوصول قرح مەل حنمت نيذل نومدختسمل
  - To: ميلإ لوصولاب حامسلا تدرأ يذلا قيبطتلا
  - Endpoint Requirements: (يضارتفالا)

Specify Access     Specify which users and endpoints can access which resources. Help      Action	
Allow     Allow     Allow specified traffic if security requirements     are met.     Block     Block	
From Specify one or more sources.	To Specify one or more destinations.
Any	Private Resources - SplunkSophos ×
Information about sources, including selecting multiple sources. Help 🖸	Information about destinations, including selecting multiple destinations. Help 🗗
Endpoint Requirements If endpoints do not meet the specified requirements for zero-trust connections, this rule will not match the t	raffic. Help 🗗
Zero-Trust Client-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is installed. Profile: System provided (Client-based)   Requirements: Disk encryption, Operating System, Endpoint	security agent, Firewall
Private Resources: SplunkSophos	
Zero Trust Browser-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is NOT installed. Profile: System provided (Browser-based)   Requirements: Operating System, Browser	~
Private Resources: SplunkSophos	

لوصولا ديدحت - لوصولا ةسايس - نمآلا لوصولا



وأ ،(Intrusion Prevention (IPS نيك متب مقت مل ،ةلاحل هذه يف نكل ،ةجاحل بسح Intrusion Prevention (IPS) وأ Tenant Control Profile.

• كيدلو، Save رقنا:

	<b>#</b> (i)	Rule name	Access	Action	Sources	Destinations	Security	Status	
8	6	Splunksophos	Private	Allow	Any	SplunkSophos	-	0	
	 		la sa l						

لوصولا ةسايس نيوكت مت - نمالا لوصولا

# Verify. ةوطخلا ةعباتم كنكمي ،كلذ دعب

# ةحصلا نم ققحتلا

<u>- چماربل لېزنت</u> نم ەليزنت كنكمي يذلا Cisco Secure Client ليمع تيبثتب تمق دق نوكت نأ بجي ،لوصولا نم ققحتلل <u>Cisco Secure Client</u>.

VPN-ار

Cisco Secure Client Agent-VPN. لالخ نم لوخدلا ليجست

🔇 Cisco Secur	Sisco Secure Client					
	AnyConnect VPN: Ready to connect. 7.vpn.sse.cisco.com	~	Connect			
	Zero Trust Access: Registration is required to access secure resources.		Enroll			
\$ ①				altalta cisco		

Secure Client - VPN

SSO رفوم لالخ نم ةقداصملا

3	Cisco	Secure	Client -	Login
---	-------	--------	----------	-------



\_

 $\times$ 

VPN - SSO - نمآلا لوصولا

• دروملا ىل لوصول كنكمي ،كتقداصم متت نأ دعب

> Login   Splunk	× +	S Cisco Secure Client	- 0	×
▲ Not secure   192	2.168.0.40:8000 en-US/act mory_id=0:Fiseisession(cost) sossi/Ff6a0Fiseirri, id= sossi/Ff6a0Fiseirri, id= fittp://buttercup-shopping.com/ fittp://buttercup-shopping.com/ fittp://buttercup-shopping.com/ fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte: fitte:	court 22 40 40 40 40 40 40 40 40 40 40	nect VPN: d to TS Remaining) If JST Access: ion is required to access sources. Enroll	2v4
		♥ ① splunk>ent	terprise Password	-liele čisco Sign In
		First time signing in?	MULTIN SESSIONED-SUSSI 77F630F65 HTTP: 1, UT 21	

قدصم - VPN - نمآلا لوصولا

Monitor > Activity Search:ىلإ لقتنا

42 Total	Viewing activity from Nov 22, 2023 1:0 23, 2023 1:09 AM	19 AM to Nov Page: 1 ▼ Results per page	50 - 1 - 42 of 42	Event Details
Request	Source	Rule Identity (2)	Destination Destinatio	Allowed
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	Nov 23, 2023 1:09 AM
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	Rule Name RDP (373192)
FW	1 vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	Source
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	Source IP
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	192.168.50.130
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	Destination IP 192.168.0.40
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	Source Port
FW	vpn user (vpnuser@ciscosspt.es)	▲ vpn user (vpnuser@ciscosspt.es)	192.168.0.4	50226
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	Destination Port 8000
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	··· Categories
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	Uncategorized Dispute Categorization
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)	192.168.0.4	

RA-VPN - طاشنلا نع ثحبلا - نمآلا لوصول

RA-VPN. لالخ نم قدصي نأ حمسي ناك لمعتسملا ىري نأ عيطتسي تنأ

## يساسألا-ليمعلا ZTNA

نم نمآ ليمع ليكو لالخ نم لوخدلا ليجست Cisco - ZTNA.



Secure Client - ZTNA

• كب صاخلا مدختسملا مساب ليجستلا.

S Cisco Secure Client - Zero Trust Access		-	×
	cisco Cisco Secure Access		
	Sign In to Enroll		
	Use your company email address and continue.		
	Email Address		
	you@yourcompany.com		
	Continue		

ليجستلا - ZTNA - نمآلا ليمعلا

SSO رفوم يف ةقداصملا

Scisco Secure Client - Zero Trust Access		 -	×
	Single Sign-On vpnuser@ciscosspt.es_edit		
	Password		
	Secured by Duo		

SSO لوخد ليجست - SSO لوخد ليجست - SSO

# • دروملا اىل لوصول كنكمي ،كتقداصم متت نأ دعب:

Login   Splunk	× +		~
← → C ▲ No	ot secure   192.168.0.40:8000/en-US/account,	/login?return_to=%2Fen-US%2F	Ŕ
<pre>0/9 FCF0001 CALENCY_10-01FT503 64-01A3515510WID-5055C7FF6ADFF5 121" 300 1313 "https://butterc 00556FF465FF7 WITP_111" 200 20</pre>	DSESSIONED-SDISLAFFIRMOFFID HTTP 1.1" 404 720 "HTTP://UU 9 HTTP 1.1" 404 3321 "http://buttercup-shopping.com/cate up-shopping.com/cat.do?action-purchase&itemId=ES1-26≺ 23 "http://buttercup-shopping.com/cat.do?action=addtoca	Cisco Secure Client	- 🗆 X
<pre>critical control control</pre>		AnyConnect VPN:	
<pre>constitute (constitute) constitute (constitute) constitute (constitute) constitute (constitute) constitute(constitute) constitute(co</pre>		Ready to connect.	✓ Connect
	FT21 HT77 1.47 406 1407 Metter/buttercup-shopping.com/c 1 417 1.47 406 1407 Metter/buttercup-shopping.com/c 1 417 / Category screen/category 14-5URPRISEASESSICATO 2 417 14000000000000000000000000000000000		
	splunk>ente	Zero Trust Access: Zero Trust Access is active.	
	Username		
	First time signing in?	* 0	
		✿ U	cisco

لجسم - ZTNA - نمآلا لوصولا

Monitor > Activity Search:ىلإ لقتنا

	- thu and (thundo) @nincondrine)	Action
FW	vpn user (vpnuser@ciscosspt.es)	Allowed
FW	vpn user (vpnuser@ciscosspt.es)	Time Nov 23, 2023 1:27 AM
FW	vpn user (vpnuser@ciscosspt.es)	Rule Name
FW	vpn user (vpnuser@ciscosspt.es)	Splunksophos
FW	vpn user (vpnuser@ciscosspt.es)	Identity
FW	vpn user (vpnuser@ciscosspt.es)	vpn user (vpnuser@ciscosspt.es)
FW	vpn user (vpnuser@ciscosspt.es)	Policy or Ruleset Identity
FW	vpn user (vpnuser@ciscosspt.es)	- Fri and ( ) Frinzel ( ) Goldson ( )
FW	vpn user (vpnuser@ciscosspt.es)	Resource/Application SplunkSophos
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	OS win 10.0.19045.3693
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	Location
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	US
ZTNA CLIENT-BASED	vpn user (vpnuser@ciscosspt.es)	Location IP 47.185.249.220
FW	vpn user (vpnuser@ciscosspt.es)	
FW	vpn user (vpnuser@ciscosspt.es)	Enpoint Security Agent windows-defender[]
FW	vpn user (vpnuser@ciscosspt.es)	Firewall
WEB	vpn user (vpnuser@ciscosspt.es)	System
WEB	vpn user (vpnuser@ciscosspt.es)	enabled[]
FW	vpn user (vpnuser@ciscosspt.es)	Disk Encryption
FW	vpn user (vpnuser@ciscosspt.es)	None
FW	vpn user (vpnuser@ciscosspt.es)	
WEB	vpn user (vpnuser@ciscosspt.es)	

العمام عن المراجع المراجع

لالخ نم قدصي نأ حمسي ناك لمعتسملا نأ تيأر عيطتسي تنأ ZTNA baser.

ضرعتسملا ىلإ دنتسملا ZTNA

ىل لوصحل URL، ىل القتنال بجي Resources > Private Resources.



SplunkSophos - صاخ دروم - نمآلا لوصول

لفسأل ريرمت •



ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما