

VPN CVR100W هجوم ىلع مدقتم ال VPN دادع

فدهل

تاكبش ال ىلع ةيها نال طاقن لي صوتل (VPN) ةيره اظلا ةصاخلا ةكبش ال مادختسا متي نيمدختسم ل ةزيمل هذه حيتت. تنرتن ال لثم، ةماع ةكبش ربع اعمة فل تخم ال. تنرتن ال ربع نام اب ةكبش ال لاصتال ةي لحم ال ةكبش ال نع نيدي عب ال نيدي عب ال.

VPN هجوم ىلع ةمدقتم ال VPN ةكبش نيوكت ةيفي ك لاقم ال اذه حرشي [ىلع ىس اس ال VPN دادع](#) ةلاقم ال ىل ع جرا، ىس اس ال VPN دادع ىلع لوصحلل CVR100W. [VPN CVR100W هجوم](#)

قيبطت لل ةلباق ال ةزه ال

VPN CVR100W هجوم

جمار بل رادص

•1.0.1.19

مدقتم ال VPN دادع

ةي لوال تاداد ال

مدقتم ال VPN دادع ال ةي لوال تاداد ال نيوكت ةيفي ك عارج ال اذه حرشي

VPN > دادع | VPN رتخاو بيول نيوكت ل ةدعاسم ال ةادل ال ىل لوخدل ل جس 1. ةوطخل
مدقتم ال VPN دادع | ةحفص رهظت. مدقتم ال

Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

IKE Policy Table

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							

VPN Policy Table

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>							

[IPSec Connection Status](#)

ةناخ دح، VPN لاصتال (NAT) ةكبش ال ناو نع ةمجرت زاي تج ني كمتل (ي رايتخ). 2. ةوطخل
ني ب VPN لاصتال عارج اب NAT زاي تج حمسي. NAT زاي تج ل قح ي **enable** رايتخ ال
ةباوب ربع رمي كي دل VPN لاصتال ناك اذا رايتخ ال اذه رتخا. NAT مدختست يتل تاباوب ال
مدت NAT.

ةكبش لل ىس اس ال عارج ال/ال خ ال ماظن ثب تايل مع ني كمتل (ي رايتخ). 3. ةوطخل
ل قح ي **enable** رايتخ ال ةناخ دح، VPN لاصتال ل الخ نم اهل اس را متيس يتل (NetBIOS)

نمضض ععبب لاصتاللا ةنالكما نيفيضم لل NetBIOS حيتي NetBIOS. ةكبش LAN.

IKE ءهن تاداع

يف لاصتاللا نمأ لاصتاللا ءاشنال مدختسي لوكوتورب وه (IKE) تنرتنال حاتفم لدابت ءارجالا اذه حرشي (SA) نامأ نارتقا سسؤملا نمألا لاصتاللا اذه يمسي VPN ةكبش ةكبش لمعت يكل. نامألا همادختسا دارملا VPN لاصتاللا IKE ةسايس نيوكت ةيفي ةقباطم ةياهنلا يتطقن الكل IKE ءهن نوكت نأ بءي، ءيحص لكشب VPN.

Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

IKE Policy Table

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							

VPN Policy Table

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>							

IPSec Connection Status

ريغتت. ءيء IKE ءهن ءاشنال فص ةفاضل قوف رونا، "IKE ءهن لوءء" يف 1. ةوطءلا مءقتملا VPN ءاعء ءءص

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

Respondent Mode: Respondent
 Auto Manual

Local ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)
 Auto Manual

Remote ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)
 Auto Manual

Redundancy Remote ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

DPD Delay: Seconds (Range: 10 - 999, Default: 10)

DPD Timeout: Seconds (Range: 30 - 1000, Default: 30)

IKE جهنل امسا لخدأ، "جهنل امسا" ل قح ي ف 2. ةوطخل

لمع ةيفي ك ديحتل ارايخ رتخأ، Exchange عضو ةلدسنم ال ةمئاق ال نم 3. ةوطخل
 ةساي س IKE.

نم أطبأ ه نإ. نامأل نم ربكأ ردق ب لمع ال IKE ةساي سل رايل ال اذه حيتي - يسي ئر
 تچتخا نو كي لي صوت VPN نم أي ري ثك نإ رايل اذه ترتخأ. طشنل اعضولا

عرس ب لمع ال ةراضل اجمار ب ال نم ةي امحل ةساي سل رايل ال اذه حيتي — ةي ن او د
 ال ةجاج كانه تنك اذا رايل ال اذه رتخأ. يسي ئر ل اعضولا نم انام لقا اهنكلو ةقئاف
 عرسأ VPN لاصتا

مت اذا. **بيجتسم ال** رايل ال ةناخ دح، بيجتسم ال عضو ني كمتل (يرايل ا). 4. ةوطخل
 نم طقف VPN ب ل ط ملتسي نأ VPN CVR100W ه جومل نكم ي ف، ةباجتس ال اعضو ني كمت
 ةدي ب ال VPN ةي اهن ةطقن

في رعتل هي ف بوغرمل اءاقتن ال رزى ل ع رقنا، يلحم ال فرم ال ل قح ي ف 5. ةوطخل
 يلحم ال فرم ال ديحت ةيفي ك

يلحم ال فرم ال ني عيتب اي ئاقتل رايل ال اذه موق ي — ي ئاقتل

اي ودي يلحم ال فرم ال ني عيتل رايل ال اذه ما دختس ا متي — ي ودي

في رعتل ةقيرط رتخأ، يلحم فرم ةلدسنم ال ةمئاق ال نم (يرايل ا). 6. ةوطخل

ة. لىل ءبش لل ءب و ل ط م ل

م اع IP ن اون ع ءط س اوب ءى ل ءم ل ءبش لل راي ءل اذ ء ءءى — IP ن اون ع

ءبش لل فى رءء ل (FQDN) ل م اك ل اب له ءم ل اءم م سا راي ءل اذ ء مءءء سى — FQDN ءى ل ءم ل

ل اءءال ءمءى . domain name و ا ن اون ع ل ا م ا ، ل اءم id لى ل ءم ل فى (ى رايءءا) . 7 ءوط ء ل ءءى 6 ءوط ءل فى راءءم ل راي ءل لى

لى ع فرءء لل ب و ل ط م ل وى ءار ل رز ق و ف ر ق ن ا ، "ءى ع ب ل فرءم ل" ل ق ء فى . 8 ءوط ءل ءى ع ب ل فرءم ل ءى ءء ءى فى ء

ءى ع ب فرءم نى ءى ع ءب اى ءءا ق ل ء راي ءل اذ ء م و قى — ى ءءا ق ل ء

اى و ءى ءى ع ب فرءم نى ءى ع ءل راي ءل اذ ء م اءءء س ا م ءى — ى و ءى

فى رءء ل ءق ى ر ط ر ءء ا ، ءى ع ب فرءم ءل ءس ن م ل ءم ءءا ق ل ن م (ى رايءءا) . 9 ءوط ءل ءى ع ب ل ءبش لل ءب و ل ط م ل

م اع IP ن اون ع ءط س اوب ءى ع ب ل ءبش لل راي ءل اذ ء ءءى — IP ن اون ع

ءبش لل لى ع فرءء لل (FQDN) ل م اك ل اب له ءم ل اءم م سا راي ءل اذ ء مءءء سى — FQDN ءى ع ب ل

ءمءى . domain name ل و ا ن اون ع ل ا م ا ، ل اءم id ءى ع ل فى (ى رايءءا) . 10 ءوط ء ل ءءى 9 ءوط ءل فى راءءم ل راي ءل لى

ءى ءء ل ب و ل ط م ل وى ءار ل رز لى ع ر ق ن ا ، ءى ع ب ل رار ءء ل فرءم ل ق ء فى . 11 ءوط ءل لى ءب ءى ع ب فرءم و ء رار ءء ل ءى ع ب ل فرءم ل . ءى ع ب ل رار ءء ل فرءم ءى ءء ءى فى ء ءى ع ب ل ءب و ل ط م ل فى VPN ق ف ن ءاءءال مءءء سى

رار ءء ل ل ءى ع ب فرءم نى ءى ع ءب اى ءءا ق ل ء راي ءل اذ ء م و قى — ى ءءا ق ل ء

اى و ءى رار ءء ل ل ءى ع ب فرءم نى ءى ع ءل راي ءل اذ ء م اءءء س ا م ءى — ى و ءى

ءق ى ر ط ر ءء ا ، رار ءء ل ل ءى ع ب ل فرءم ل ءل ءس ن م ل ءم ءءا ق ل ن م (ى رايءءا) . 12 ءوط ءل رار ءء ل ءبش لل ءب و ل ط م ل فى رءء ل

م اع IP ن اون ع ءط س اوب ءى ط اى ءءا ل ءى ع ب ل ءبش لل راي ءل اذ ء ءءى — IP ن اون ع

ءبش لل ءى ءء ل (FQDN) ل م اك ل اب له ءم ل اءم م سا راي ءل اذ ء مءءء سى — FQDN رار ءء ل ل ءى ع ب ل

ل اءم ل م سا و ا IP ن اون ع ل اءءا ، ءى ع ب ل رار ءء ل فرءم ل ق ء فى (ى رايءءا) . 13 ءوط ءل 12 ءوط ءل فى راءءم ل راي ءل لى

IKE SA Parameters	
Encryption Algorithm:	AES-128 ▼
Authentication Algorithm:	SHA-1 ▼
Pre-Shared Key:	1234abcd
Diffie-Hellman (DH) Group:	Group1 (768 bit) ▼
SA-Lifetime:	3600 Seconds (Range: 30 - 86400, Default: 3600)
Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	10 Seconds (Range: 10 - 999, Default: 10)
DPD Timeout:	30 Seconds (Range: 30 - 1000, Default: 30)

يلع ضوافتلل ارايخ رتخأ، ريفشتللا ةيمزراوخل ةلدسنملا ةمئاقلا نم 14. ةوطخل (SA) نامألا نارثقا

· ريفشتل تب 56 حاتفم مجح (DES) تانايبلا ريفشتل رايعم مدختسي — DES. طقف DES معدت ةدحاو ةياهن ةطقن تناك اذا همادختسا بجيو ميديق DES. تانايبلا

· تارم ثالث DES رايعم لبا (3DES) تانايبلا ريفشتل يثالثلا رايعم لبا لمعي — 3DES. ةلوج بسح تب 56 لىلى تب 112 نمو تب 112 لىلى تب 168 نم حاتفملا مجح ريغي هنكلو AES و DES نم انامأ رثكأ 3DES نوكت. اهذيفنت متي يتلا DES.

· حاتفم (AES-128) تب-128 حاتفم عم مدقتملا ريفشتل رايعم مدختسي — AES-128. انماو ةعرس رثكأ هئاب (AES) روطتملا ريفشتل ماظن زيمني. AES ريفشتل تب-128 نوكي نأ 3DES حيتت ةزهجال اعاونأ ضعب. (DES) روطتملا ريفشتل فاشتك ماظن نم AES-256 و AES-192 نيزارطال نم انامأ لقا هنكلو ةعرس رثكأ AES-128 زارطال. عرسا

· AES-192 زارطال زيمني. AES ريفشتل تب-192 حاتفم AES-192 مدختسي — AES-192 زيمني AES-192 زارطال نأ امك، AES-128 زارطال نم انامأ رثكأ هنكلو ائطب رثكأ هئاب AES-256 زارطال نم انامأ لقا هنكلو ربكأ ةعرسب

· AES-256 زارطال زيمني. AES ريفشتل تب-256 حاتفم AES-256 مدختسي — AES-256 AES-192 و AES-128 نيزارطال نم انامأ رثكأ هنكلو ائطب رثكأ هئاب

VPN. سار ةقداصملا ارايخ رتخأ، ةقداصملا ةيمزراوخل ةلدسنملا ةمئاقلا نم 15. ةوطخل

· ةقداصملا تب 128 ةئجت ةميقي مدختست (MD5) 5 ةلاسرا صخلم ةيمزراوخ — MD5. SHA-1 و SHA2-256 نيزارطال نم عرسا هنكلو انامأ لقا MD5 زارطال

· تب 160 ةئجت ةميقي (SHA-1) 1 ةنمألا ةئجتلا ةيمزراوخ مدختست — SHA-1 زارطال نأ امك، MD5 زارطال نم انامأ رثكأ هنكلو ائطب SHA-1 زارطال دعوي. ةقداصملا SHA2-256 زارطال نم انامأ لقا هنكلو ةعرس رثكأ SHA-1

· تب 256 ةئجت ةميقي (SHA2-256) 2 ةنمألا ةئجتلا ةيمزراوخ مدختست — SHA2-256 SHA-1 و MD5 نم نم ائطب SHA2-256. ةقداصملا

همدختسي اقبسم كرتشم حاتفم لخدا، "اقبسم كرتشم حاتفم" لقي في 16. ةوطخل IKE. جهن

يتلا DH ةعومجم رتخأ، Diffie-Hellman (DH) ةعومجملا ةلدسنملا ةمئاقلا نم 17. ةوطخل

ة فرعم نود حيت افملا لدابت DH ةومجم يف ني فيضملل نكمي. IKE اهمدختست انام ارثك ةومجملا تناك ام لك ، ةومجملا تب مقرر دارم لك . ضعب ل مهضعب

VPN ل (SA) نارتقا ةينمألا (يناوثلاب) ةدملا ام ، لاجم SA-Lifetime ل يف تلخد . 18 ةوطخل SA دي دجت متي نأ لبق يقبي

رايتخالال ةناخ دح ، (DPD) فقوتملا ريظنلا فاشتكلا ني كمتل (يرايتخال) . 19 ةوطخل IKE ءارظن ةبقارملا DPD مدختسي . فقوتملا ريظنلا فاشتكلا ل قح يف **enable** نارقألا لعل ةكبشلا دراوم راده DPD عنمي . لمعلال نع ريظنلا فقوت اذا ام ققحتلل ني طشانلا ريغ

لصافلا ، طاشنلل ريظنلا صحف متي ةرم مك ل ريشي نأ (يرايتخال) . 20 ةوطخل لدي يف احاتم DPD ناك اذا احاتم رايتخال اذه نوكي . DPD ريخات ل قح يف (يناوثلاب) ينمزلل 19 ةوطخل

ريغ ريظنلا طاقس متي نأ لبق رظنتي نأ يتم ل ريشي نأ (يرايتخال) . 21 ةوطخل لدي DPD ناك اذا احاتم رايتخال اذه نوكي . DPD ةلهم ل قح يف (يناوثلاب) لوط وه ام ، طشانلا 19 ةوطخل يف احاتم

يرخا ةرم ةيلصألا ةمدقتملا VPN دادع ةحفص رهظت . ظفح ةقطق . 22 ةوطخل

IKE Policy Table							
<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input checked="" type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

Add Row Edit Delete

ةصاخلا رايتخالال ةناخ دح ، IKE جهن لودج يف IKE ةسايس ريحتل (يرايتخال) . 23 ةوطخل ظفح قوف رقناو ، ةبولطملا لوقحلا ريحتب مقو ، ريحت قوف رقنا م . جهنلاب

جهنلل رايتخالال ةناخ دح ، IKE ةسايس لودج يف IKE ةسايس فذحل (يرايتخال) . 24 ةوطخل ظفح قوف رقنا م . فذح قوف رقناو

VPN جهن تادادع

هم ادختس متيس يذلا VPN لاصلتال VPN ةسايس نيوكت ةيفي ك ءارجل اذه حرشي ال كل VPN ةكبش تاسايس نوكت نأ بجي ، حيحص لكشب VPN ةكبش لمعت يكل ةقباطم ةياهنلا يتطقن .

Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

IKE Policy Table							
<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

Add Row Edit Delete

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

ةسايس ءاشنل فص ةفاضل قوف رقنا ، "VPN ةكبش ةسايس لودج" يف 1 ةوطخل م دقتملا VPN دادع ةحفص ريغتت . ةدي دج VPN ةكبش

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

(Hint: 1.2.3.4 or abc.com)

Rollback enable

Local Traffic Selection

Local IP:

IP Address:

(Hint: 1.2.3.4)

Subnet Mask:

(Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

IP Address:

(Hint: 1.2.3.4)

Subnet Mask:

(Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Auto Policy Parameters

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type: ▼

Remote Endpoint: ▼

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

▼

(Hint: 1.2.3.4 or abc.com)

Rollback enable

VPN جهنل امسا لخدأ ، "جهنل امسا" ل قح يف 2. ةوطخل

تادادع| ءاشن ة يفك ديدحتل ارايخ رتخأ ، "جهنل اعون" ةلدسنملا ةمئاقلا نم 3. ةوطخل
 قف VPN.

تانايبل ريفش تب ةصاخلا حيتافملا نيوكت رايلال اذه كل حيتي — يودي جهن.
 اهتمالسو

اهريفش وتانايبل ةمالسل IKE ةسايس رايلال اذه مدختسي — يئاقلت جهن.
 حيتافملا لدابت تايلمعل

ة يفك ديدحتل ارايخ رتخأ ، "ةديعبلا ةياهنلا ةطقن" ةلدسنملا ةمئاقلا نم 4. ةوطخل
 ايلودي ديعبل فرعما صيصخت

ماع IP ناوع ةطساوب ةديعبلا ةكبشلا رايلال اذه دحي — IP ناوع.

ةكبشلا لىل فرعتلل (FQDN) لمالكاب لهؤم لاجم مسا رايلال اذه مدختسي — FQDN.
 ةديعبلا

"ةديعبلا ةياهنلا ةطقن" ةلدسنملا ةمئاقلا لفسأ صنلا لاخدإ ل قح يف 5. ةوطخل
 ديعبل ناوعلل لاجملا مسا و ماعلا IP ناوع اما لخدأ

ةياهن ةطقن ل قح يف نيكم ت رايلال ةناخ دح ، راركتل نيكم تل (يرايخ). 6. ةوطخل
 لاصتالا ةينام VPN CVR100W هجومل راركتلا ةياهن ةطقن رايلال حيتي . راركتلا
 يساسالا VPN لاصتلا لشف دن ةيطايلح VPN ةياهن ةطقن

ةلدسنملا ةمئاقلا نم ارايخ رتخأ ، ايلودي راركتل فرعم نييعلتل (يرايخ). 7. ةوطخل
 راركتلا ةياهن ةطقن

ماع IP ناوع ةطساوب ةيطايلحال ةديعبلا ةكبشلا رايلال اذه دحي — IP ناوع.

ةكبشلا ديدحتل (FQDN) لمالكاب لهؤم لاجم مسا رايلال اذه مدختسي — FQDN.
 راركتلل ةديعبلا

ةمئاقلا لفسأ صنلا لاخدإ ل قح يف ، راركتلا ناوع لاخدإ (يرايخ). 8. ةوطخل
 لاجملا مسا و ماعلا IP ناوع اما لخدأ ، راركتلا ةياهن ةطقن ةلدسنملا

رايلال اذه نكمي . عجارتل نيكم ت رايلال ةناخ دح ، عجارتل نيكم تل (يرايخ). 9. ةوطخل
 لاصتالا ليطايلحال (VPN) ةيرهاظلا ةصاخلا ةكبشلا لاصتلا نم يئاقلتلا ليوحتلا

ةكبشلا لاصتا دادرستسا مت دق نوكي ام دنع ياساسألا (VPN) ةرهظلا ةصاخلا ةكبشلا لشف نم ياساسألا (VPN) ةرهظلا ةصاخلا.

Local Traffic Selection		
Local IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="192.168.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.255.255.0"/>	(Hint: 255.255.255.0)
Remote Traffic Selection		
Remote IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="10.1.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.0.0.0"/>	(Hint: 255.255.255.0)

ةفضملا تائيبلا ديدحتل ارايخ رتخأ، ةيلحملا IP ةلدسنملا ةمئاقلا نم 10. ةوطخلا ةسايسلاب رثأتت يتلا.

ةيلحم VPN لاصتا ةطقنك دحاو ففضم رايخلا اذه مدختسي — يداحأ.

ةطقنك ةيلحملا ةكبشلا نم ةيعرف ةكبش رايخلا اذه مدختسي — ةيعرفلا ةكبشلا ةيلحم VPN لاصتا.

ففضملا وأ ةيعرفلا ةكبشلا ل IP ناو نع وأ ففضملا لخدأ، IP ناو نع لققح يف 11. ةوطخلا ةيلحملا.

عانق لخدأف، 10. ةوطخلا يف ةيعرفلا ةكبشلا رايخ رايختخا مت اذا (يرايتخا). 12. ةوطخلا ةيعرفلا ةكبشلا عانق لققح يف ةيلحملا ةيعرفلا ةكبشلا ل ةيعرفلا ةكبشلا.

ةفضملا تائيبلا ديدحتل ارايخ رتخأ، ةديعبلا IP ةلدسنملا ةمئاقلا نم 13. ةوطخلا ةيلحملا رثأتت يتلا.

ةديعبلا VPN لاصتا ةطقنك ادحاو ففضم رايخلا اذه مدختسي — يداحأ.

ةطقنك ةديعبلا ةكبشلا ل ةيعرف ةكبش رايخلا اذه مدختسي — ةيعرفلا ةكبشلا ةديعبلا VPN لاصتا.

ففضملا وأ ةيعرفلا ةكبشلا ل IP ناو نع وأ ففضملا لخدأ، IP ناو نع لققح يف 14. ةوطخلا ةديعبلا.

عانق لخدأف، 13. ةوطخلا يف ةيعرفلا ةكبشلا رايخ رايختخا مت اذا (يرايتخا). 15. ةوطخلا ةيعرفلا ةكبشلا عانق لققح يف ةديعبلا ةيعرفلا ةكبشلا ل ةيعرفلا ةكبشلا.

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="0xABCD"/>
SPI-Outgoing:	<input type="text" value="0x1234"/>
Encryption Algorithm:	<input type="text" value="AES-128"/>
Key-In:	<input type="text" value="12345678ABCDE"/>
Key-Out:	<input type="text" value="12345678ABCDE"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/>
Key-In:	<input type="text" value="12345678ABCD"/>
Key-Out:	<input type="text" value="12345678ABCD"/>

16 ةوطخلال ذيفنتب مقف ،3 ةوطخلال يف ةيوديلا ةسايسلا راڤ رايتخا مت اذا :**ةطخال م** [24 ةوطخال](#) لىل يطيختلاب مقف ،الو ؛23 ةوطخلال ح

ةيرشع ةيسادس فورح ةينامث لىل ةثالث نم لخدأ ،SPI-Incoming لقح يف 16 ةوطخلال لىل VPN لاصتا لىل ةدراول رورملا ةكرحل (SPI) نامأل تاملعم سرهف ةمالعل بچي .ةسلج رخآ نم رورم ةكرحل نم ةسلج دحاو نم رورم ةكرحل زيمي نا ةقاطب تلمعتسا قفنل نم رخآل بناجل لىل رداصل SPI قفنل نم بناج لىل دراول SPI نوكي نا

ةيرشع ةيسادس فورح ةينامث لىل ةثالث نم لخدأ ،SPI-Outgoing لقح يف 17 ةوطخلال زيمي نا ةقاطب تلمعتسا لىل VPN لاصتا لىل ةدراول رورملا ةكرحل SPI ةمالعل لىل رداصل SPI نوكي نا بچي .ةسلج رخآ نم رورم ةكرحل نم ةسلج دحاو نم رورم ةكرحل قفنل نم رخآل بناجل لىل دراول SPI وه قفنل يبناج دح

لىل ضوافتلل ارايخ رتخأ ،ريفشتلل ةيمزراوخل ةلدسنملا ةمئاقلا نم 18 ةوطخلال (SA) نامأل نارثقا

ريفشتل تب 56 حاتفم مچح (DES) تانايبلا ريفشتل رايعم مدختسي — DES .طقف DES معدت ةدحاو ةياهن ةطقن تناك اذا همادختسا بچي وميدق DES .تانايبلا

تارم ثالث DES رايعملا ب (3DES) تانايبلا ريفشتل يثالثلا رايعملا لمعي — 3DES .ةلوج بسح تب 56 لىل تب 112 نمو تب 112 لىل تب 168 نم حاتفملا مچح ريغي هنكلو AES و DES نم انامأ رثكأ 3DES نوكت .اهذيفنت متي يتل DES

حاتفم (AES-128) تب-128 حاتفم عم مدقتملا ريفشتل رايعم مدختسي — AES-128 .3DES نكمت ةزهجال عاونأ ضع ب .DES نم انامأ رثكأ أو عرسأ AES .AES ريفشتل تب-128 و AES-192 ني زارطلال نم انامأ لقا هنكلو ةعرس رثكأ AES-128 زارطلال .عرسأ نوكي نا نم AES-256.

AES-192 زارطلال زيمي تي .AES ريفشتل تب-192 حاتفم AES-192 مدختسي — AES-192 زيمي تي AES-192 زارطلال نا امك ،AES-128 زارطلال نم انامأ رثكأ هنكلو ائطب رثكأ هنأب AES-256 زارطلال نم انامأ لقا هنكلو ربكأ ةعرسب

AES-256 زارطلال زيمي تي .AES ريفشتل تب-256 حاتفم AES-256 مدختسي — AES-256 AES-192 و AES-128 ني زارطلال نم انامأ رثكأ هنكلو ائطب رثكأ هنأب

لىل حاتفملا لوط دمتعي .دراول جهنلل حاتفم ،لاجم لخد حاتفملا يف تلخد 19 ةوطخلال 18 ةوطخلال يف ةراتخملا ةيمزراوخل

· فرحاً 8 نم نوكم حاتفم DES مدختسي.

· افرح 24 نم نوكم حاتفم 3DES رايعم مدختسي.

· افرح 12 نم نوكم حاتفم AES-128 زارطلال مدختسي.

· افرح 24 نم نوكم حاتفم AES-192 زارطلال مدختسي.

· افرح 32 نم نوكم حاتفم AES-256 زارطلال مدختسي.

حاتفملا لوط دمتعي. رداصلال جهنلل حاتفم، لاجم جراخ حاتفملا يف تلخد. 20 ةوطخلال
ةراتخملا ةيمزراوخلال لعل حاتفملا لوط دمتعي. 18 ةوطخلال يف ةراتخملا ةيمزراوخلال لعل
18 ةوطخلال يف.

· فرحاً 8 نم نوكم حاتفم DES مدختسي.

· افرح 24 نم نوكم حاتفم 3DES رايعم مدختسي.

· افرح 12 نم نوكم حاتفم AES-128 زارطلال مدختسي.

· افرح 24 نم نوكم حاتفم AES-192 زارطلال مدختسي.

· افرح 32 نم نوكم حاتفم AES-256 زارطلال مدختسي.

VPN سار ةقداصلمل ارايخ رتخأ، لمالك تلال ةيمزراوخل ةلدسنملا ةمئاقلا نم. 21 ةوطخلال

· ةقداصلمل تب 128 ةئزجت ةميق مدختست (MD5) 5 ةلاس رلا صخلم ةيمزراوخ — MD5.
SHA-1 و SHA2-256 ني زارطلال نم عرساً هنكلو نامال نم لقا رقب MD5 زارطلال زي متي.

· تب 160 ةئزجت ةميق (SHA-1) 1 ةنمآلا ةئزجت تلال ةيمزراوخ مدختست — SHA-1
زارطلال نامك، MD5 زارطلال نم انامأ رثكأ هنكلو أطبأ SHA-1 زارطلال دعيو. ةقداصلمل
SHA2-256 زارطلال نم انامأ لقا هنكلو عرس رثكأ SHA-1.

· تب 256 ةئزجت ةميق (SHA2-256) 2 ةنمآلا ةئزجت تلال ةيمزراوخ مدختست — SHA2-256
و MD5 ني زارطلال ةنراقم انامأ أو اطب رثكأ هنأب SHA2-256 زارطلال زي متي. ةقداصلمل
SHA-1.

لعل حاتفملا لوط دمتعي. دراوال جهنلل حاتفم، لاجم لخاد حاتفملا يف تلخد. 22 ةوطخلال
21 ةوطخلال يف ةراتخملا ةيمزراوخلال

· فرح 16 نم نوكم فرح حاتفم MD5 زارطلال مدختسي.

· فرح 20 نم نوكم حاتفم SHA-1 مدختسي.

· افرح 32 حاتفم SHA2-256 مدختسي.

حاتفملا لوط دمتعي. رداصلال جهنلل حاتفم، لاجم جراخ حاتفملا يف تلخد. 23 ةوطخلال
ةراتخملا ةيمزراوخلال لعل حاتفملا لوط دمتعي. 21 ةوطخلال يف ةراتخملا ةيمزراوخلال لعل
21 ةوطخلال يف.

· فرح 16 نم نوكم فرح حاتفم MD5 زارطلال مدختسي.

· فرح 20 نم نوكم حاتفم SHA-1 مدختسي.

· افرح 32 حاتفم SHA2-256 مدختسي.

Auto Policy Parameters

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

يحتوي 24 عوطل على ذي فنن ت ب مقف ، 3 عوطل على في ة ئاق ل لت ال ة سا ي س ال ت رتخ اذ : **عطل ال م** [31 عوطل](#) ال ال ي ط خ ت ل اب مقف ، ال او ؛ 29 عوطل ال

SA ال ا هي ف ر م ت س ت ي ت ال ة د م ال ل خ د ا ، SA ل ي ض ا ر ت ف ال ر م ع ال ل ق ح ي ف . 24 عوطل ال د ي د ج ت ال ل ب ق ي ن او ث ل اب

ل ع ض و ا ف ت ل ل ا ر ا ي خ ر ت خ ا ، ر ي ف ش ت ال ة ي م ز ر ا و خ ل ة ل د س ن م ال ة م ئ ا ق ل ال م . 25 عوطل ال (SA) ن ا م ال ن ا ر ت ق ا

• ر ي ف ش ت ل ت ب 56 ح ا ت ف م م ج ح (DES) ت ا ن ا ي ب ال ر ي ف ش ت ر ا ي ع م م د خ ت س ي — DES . ط ق ف DES م ع د ت ة د ح ا و ة ي ا ه ن ة ط ق ن ت ن ا ك ا ذ ا ه م ا د خ ت س ا ب ج ي و م ي د ق DES . ت ا ن ا ي ب ال

• ت ا ر م ث ا ل ت DES ر ا ي ع م ل اب (3DES) ت ا ن ا ي ب ال ر ي ف ش ت ل ي ث ا ل ث ال ر ا ي ع م ال ل م ع ي — 3DES . ة ل و ج ب س ح ت ب 56 ال ت ب 112 ن م و ت ب 112 ال ت ب 168 ن م ح ا ت ف م ال م ج ح ر ي غ ي ه ن ك ل و AES و DES ن م ا ن ا م ا ر ث ك ا 3DES ن و ك ت . ا ه ذ ي ف ن ت م ت ي ت ال DES .

• ح ا ت ف م (AES-128) ت ب-128 ح ا ت ف م ع م م د ق ت م ال ر ي ف ش ت ال ر ا ي ع م م د خ ت س ي — AES-128 . ا ن م ا و ة ع ر س ر ث ك ا ه ن ا ب (AES) ر و ط ت م ال ر ي ف ش ت ال م ا ط ن ز ي م ت ي . AES ر ي ف ش ت ل ت ب-128 ن و ك ي ن ا 3DES ح ي ت ت ة ز ه ج ال ع ا و ن ا ض ع ب . (DES) ر و ط ت م ال ر ي ف ش ت ال ف ا ش ت ك ا م ا ط ن ن م AES-192 و AES-256 ن ي ز ا ر ط ال ن م ا ن ا م ا ل ق ا ه ن ك ل و ة ع ر س ر ث ك ا AES-128 ز ا ر ط ال . ع ر س ا

• AES-192 ز ا ر ط ال ز ي م ت ي . AES ر ي ف ش ت ل ت ب-192 ح ا ت ف م AES-192 م د خ ت س ي — AES-192 . ز ي م ت ي AES-192 ز ا ر ط ال ن ا م ك ، AES-128 ز ا ر ط ال ن م ا ن ا م ا ر ث ك ا ه ن ك ل و ا ئ ط ب ر ث ك ا ه ن ا ب AES-256 ز ا ر ط ال ن م ا ن ا م ا ل ق ا ه ن ك ل و ر ب ك ا ة ع ر س ب

• AES-256 ز ا ر ط ال ز ي م ت ي . AES ر ي ف ش ت ل ت ب-256 ح ا ت ف م AES-256 م د خ ت س ي — AES-256 . AES-192 و AES-128 ن ي ز ا ر ط ال ن م ا ن ا م ا ر ث ك ا ه ن ك ل و ا ئ ط ب ر ث ك ا ه ن ا ب

VPN س ا ر ة ق د ا ص م ل ا ر ا ي خ ر ت خ ا ، ل م ا ك ت ال ة ي م ز ر ا و خ ل ة ل د س ن م ال ة م ئ ا ق ل ال م . 26 عوطل ال

• ة ق د ا ص م ل ل ت ب 128 ة ئ ز ج ت ة م ي ق م د خ ت س ت (MD5) 5 ة ل ا س ر ل ا ص خ ل م ة ي م ز ر ا و خ — MD5 . SHA-1 و SHA2-256 ن ي ز ا ر ط ال ن م ع ر س ا ه ن ك ل و ن ا م ال ن م ل ق ا ر د ق ب MD5 ز ا ر ط ال ز ي م ت ي

• ت ب 160 ة ئ ز ج ت ة م ي ق (SHA-1) 1 ة ن م ال ة ئ ز ج ت ال ة ي م ز ر ا و خ م د خ ت س ت — SHA-1 . ز ا ر ط ال ن ا م ك ، MD5 ز ا ر ط ال ن م ا ن ا م ا ر ث ك ا ه ن ك ل و ا ط ب ا SHA-1 ز ا ر ط ال د ع ي و . ة ق د ا ص م ل ل SHA-1 و SHA2-256 ز ا ر ط ال ن م ا ن ا م ا ل ق ا ه ن ك ل و ة ع ر س ر ث ك ا SHA-1

• ت ب 256 ة ئ ز ج ت ة م ي ق (SHA2-256) 2 ة ن م ال ة ئ ز ج ت ال ة ي م ز ر ا و خ م د خ ت س ت — SHA2-256 . SHA-1 و MD5 ن م ن م ا ه ن ك ل و ا ط ب ا SHA2-256 . ة ق د ا ص م ل ل

ةداع| ةيرس نيكم تل PFS حيتافم ةعومجم ل قح يف نيكم ت رايتخال ا ةناخ دح . 27 ةوطخال اهنكل ، (VPN) ةيرهاظلا ةصخال ا ةكبشلا نامأ نم PFS ديزت . (PFS) ةلماكل ا هيجوتلا لاصلال ا ةعرس ئطبت .

28 ةوطخال Diffie-Hellman ةعومجم رتخأ ، 27 ةوطخال يف PFS نيكم ت رتخأ اذا (يراي تخأ) . 28 ةوطخال ا ناكل ام لكو . PFS حيتافم ةعومجم ل قح لفسأ ، ةلدسنملا ةمئاقلا نم امامضنلال (DH) . انامأ رثكأ ةعومجملا تناكل ام لكو ، يلعأ ةعومجملا مقرر .

هم ادختس! متيس يذلا IKE جهن رتخأ ، IKE جهن ديدحت ةلدسنملا ةمئاقلا نم . 29 ةوطخال ا VPN جهنل .

نيوكت مسق يلى كهيجوت متيس ف ، ضرع قوف رقنلاب تمق اذا (يراي تخأ) . 30 ةوطخال ا م دقتملا VPN دادع| ةحفص نم IKE .

ىرخأ ةرم ةيلصلال ا ةمدقتملا VPN دادع| ةحفص رهظت . ظفح ةق طقط . 31 ةوطخال ا

ظفح ةق طقط . 32 ةوطخال ا

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input checked="" type="checkbox"/>	Disabled	Policy1	Auto Policy	192.168.1.1/255.255.255.0	10.1.1.1/255.0.0.0	SHA-1	AES-128
Add Row Edit Enable Disable Delete							

ةصخال ا ةكبشلا ةسايس لودج يف VPN ةكبش ةسايس ريرحتل (يراي تخأ) . 33 ةوطخال ا لوقحل ريرحتب مقو ، ريرحت قوف رقنا م . جهنلل رايتخال ا ةناخ دح ، (VPN) ةيرهاظلا لظفح قوف رقناو ، ةبولطملا .

رايتخال ا ةناخ دح ، VPN ةسايس لودج يف VPN ةسايس فذحل (يراي تخأ) . 34 ةوطخال ا لظفح قوف رقنا م ، فذح قوف رقنا ، جهنلل .

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا