

FDM مادختساب جودزملا ISP نیوکت

تایوتحملا

[قمدقملا](#)

[قیس اس آلا تابل طتملا](#)

[تابل طتملا](#)

[قمدختسملا تانوكملا](#)

[نیوکتللا](#)

[قک بشیل لی طخ تللا مسدرلا](#)

[قحص لانم ققحتللا](#)

قمدقملا

جودزملا تنرتنلا اقمد خرفوم لشف زواجت نیوکت ئیفیک دنتسمل اذه حضوی نمآللا ئیامحلا رادج ئزهچأ ریدم مادختساب.

قیس اس آلا تابل طتملا

تابل طتملا

قیلاتلا عیض اوبلاب ئفرعم کیدل نوکت نأب Cisco يصوت:

- يس اس آلا هي جوتلا
- ئیامحلا رادج ئزهچأ ئرادا تامولعم ئحول ئفرعم

نمآللا ئیامحلا رادجب لق آلا ىلع تنرتن اقمد خيرفوم ليصوت مت.

قمدختسملا تانوكملا

قیلاتلا ئیدامل اتانوكملا وجماربلا تارادصا ىلإ دنتسمل اذه يف ئدراول ا تامولعملا دنتسست:

ثدح آلا تارادص إلاؤ 7.7.x رادص إلاؤ Cisco نم نمآللا ئیامحلا رادج ليغشت.

رادص إلاؤ 7.7.0 رادص إلاؤ 3130 نمآللا ئیامحلا رادج.

قصاخ ئیلمعم ئییب يف ئدوچوملا ئزهچ آلا نم دنتسمل اذه يف ئدراول ا تامولعملا عاشن ا مت تناك اذا. (يضارتفا) حوسمم نیوکتب دنتسمل اذه يف ئمدختسملا ئزهچ آلا عیمج تأدب رمأ يأ لمحتملا ریثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكب بش.

نیوکتللا

1. ئوطخلالا

رزلـا دـيـدـحـتـ لـالـخـ نـمـ تـاهـجـاـوـلـا مـسـقـىـلـا لـقـنـتـوـ،ـنـمـآـلـا ةـيـامـحـلـا رـادـجـىـلـعـ FDMـ ئـلـا لـفـخـدـلـا لـجـسـ تـاهـجـاـوـلـا عـيـمـجـ ضـرـعـ.

The screenshot shows the Firewall Device Manager interface for a Cisco Secure Firewall 3130 Threat Defense (SF3130). The top bar displays the device name 'Device: SF3130' and user information 'admin Administrator'. The main area shows the device's model, software version (7.7.0-89), VDB (408.0), and last intrusion rule update (20250605-1326). It also indicates 'Cloud Services Connected | HackaTZ-2025' and 'High Availability Not Configured'. A 'CONFIGURE' button is visible.

Network Layout:

- Inside Network:** Shows icons for MGMT (Console) and CONSOLE.
- ISP/WAN/Gateway:** Shows icons for Internet, DNS Server, NTP Server, and Smart License.
- Cloud Services:** Shows a connection to 'HackaTZ-2025'.

Interface Configuration:

- No interface named "inside".
- No interface named "outside".
- Management: Merged (Enabled 1 of 1)
- View All Interfaces (button highlighted with a red box)
- Smart License: Registered
- Backup and Restore
- Troubleshoot
- Updates: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds
- System Settings: Management Access, Logging Settings, DHCP Server / Relay, DDNS Service, DNS Server, Hostname, Time Services, SSL Settings, See more

لـ ةـيـسـيـئـرـلـا تـامـولـعـمـلـا ةـحـوـلـ FDMـ

2. ۋەطخـلـا.

ةـهـجـاـوـلـا رـزـ دـيـدـحـتـ.ـةـبـولـطـمـلـا ةـهـجـاـوـلـا دـيـدـحـتـ بـأـدـبـاـ،ـيـسـاسـأـلـا ISPـ لـاصـتـالـ ةـهـجـاـوـلـا نـيـوـكـتـلـا يـهـ ةـمـدـخـتـسـمـلـا ةـهـجـاـوـلـا Ethernet1/1ـ يـفـ.ـعـبـاتـمـلـلـ ۋـقـبـاـطـمـلـا

The screenshot shows the Firewall Device Manager interface for the same device. The top bar and user information are identical. The main area shows the device's model, software version (7.7.0-89), VDB (408.0), and last intrusion rule update (20250605-1326). It also indicates 'Cloud Services Connected | HackaTZ-2025' and 'High Availability Not Configured'. A 'CONFIGURE' button is visible.

Device Summary:

Interfaces Tab:

- Device Summary: Interfaces
- Cisco Secure Firewall 3130 Threat Defense (MGMT, CONSOLE, 1/1, 1/3, 1/5, 1/7, 1/9, 1/10, 1/11, 1/12, 1/13, 1/14, 1/15, 1/16, SFP, Network Module Not Installed)

Table View:

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
Ethernet1/1	1	<input checked="" type="checkbox"/>	Routed				
Ethernet1/2		<input checked="" type="checkbox"/>	Routed				
Ethernet1/3	2	<input checked="" type="checkbox"/>	Routed				
Ethernet1/4		<input checked="" type="checkbox"/>	Routed			Enabled	
Ethernet1/5		<input checked="" type="checkbox"/>	Routed			Enabled	
Ethernet1/6		<input checked="" type="checkbox"/>	Routed			Enabled	
Ethernet1/7		<input checked="" type="checkbox"/>	Routed			Enabled	

تـاهـجـاـوـلـا بـيـوـبـتـ ةـمـالـعـ

3. ۋەطخـلـا.

اـذـهـ يـفـ.ـكـيـدـلـ يـسـاسـأـلـا ISPـ لـاصـتـالـ ةـحـيـحـصـلـا تـامـلـعـمـلـا مـادـخـتـسـابـ ةـهـجـاـوـلـا نـيـوـكـتـبـ مـقـ

يـسـاسـأـجـراـخـنـرـاقـلـاـ،ـلـاثـمـ.

Ethernet1/1 Edit Physical Interface

Interface Name: outside_primary Mode: Routed Status: Enabled

Most features work with named interfaces only, although some require unnamed interfaces.

Description: ISP Primary

IPv4 Address IPv6 Address Advanced

Type: Static

IP Address and Subnet Mask: 172.16.1.1 / 255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask:

e.g. 192.168.5.16

CANCEL OK

يـسـاسـأـجـراـخـنـرـاقـلـاـ،ـلـاثـمـ.

4. ۋەطخـلـاـ.

ـلـاثـمـلـاـ اـذـهـ يـفـ.ـقـيـونـاـثـلـاـISPـاـجـاـولـاـ ـلـاثـمـلـاـ مـتـيـ.ـقـيـلـمـعـلـاـ سـفـنـ رـرـكـ.

Ethernet1/2

Edit Physical Interface



Interface Name

Mode

Status

outside_backup

Routed



Most features work with named interfaces only, although some require unnamed interfaces.

Description

ISP Backup



IPv4 Address

IPv6 Address

Advanced

Type

Static ▾

IP Address and Subnet Mask

172.16.2.1

/ 255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

I

e.g. 192.168.5.16

CANCEL

OK

ةيوناثل ISP ۋەجىءەن يوكتى

٥. وظائف

ةهجاولل SLA ةبقارم دادعإ يف ةيلاتلا وةوطخلال ثمت، ISPs ل تاهجاولا نيوكت دعب ةيساسألا.

مئا اقل ايلعأ يف دوجوملا تانئاكللا رز ديدحتب تانئاكللا مسق ىلإ لقتنا.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: SF3130

Device Summary
Interfaces

Interfaces | Bridge Groups | EtherChannels | Virtual Tunnel Interfaces | Inline Sets

17 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
Ethernet1/1	outside_primary	<input checked="" type="checkbox"/>	Routed	172.16.1.1			
Ethernet1/2	outside_backup	<input checked="" type="checkbox"/>	Routed	172.16.2.1			
Ethernet1/3	inside	<input checked="" type="checkbox"/>	Routed	192.168.1.1			
Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	
Ethernet1/5		<input type="checkbox"/>	Routed			Enabled	
Ethernet1/6		<input type="checkbox"/>	Routed			Enabled	
Ethernet1/7		<input type="checkbox"/>	Routed			Enabled	
Ethernet1/8		<input type="checkbox"/>	Routed			Enabled	

اهنیوکت مٽ یتلا تاھج اووا

6. ۋەطخىل.

تاشاش رز، رسىيالا دومعلا يف ددح SLA.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: SF3130

Ports

- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors**
- SGT Groups

Network Objects and Groups

8 objects

#	NAME	TYPE	VALUE
1	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16
2	Gateway-Outside-1	HOST	172.16.1.254
3	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8
4	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12
5	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16
6	Inside	NETWORK	192.168.1.0/24
7	any-ipv4	NETWORK	0.0.0.0/0
8	any-ipv6	NETWORK	::/0

تانىاكلالا ۋەشىش

7. ۋەطخىل.

ةشاش عاشنى رزلالا دىدحت قىرط نع ۋەدىدج SLA.

The screenshot shows the Firewall Device Manager interface with the following details:

- Top Bar:** Firewall Device Manager, Monitoring, Policies, **Objects** (selected), Device: SF3130.
- Left Sidebar:** Ports, Security Zones, Application Filters, URLs, Geolocations, Syslog Servers, IKE Policies, IPSec Proposals, Secure Client Profiles, Identity Sources, Users, Certificates, Secret Keys, DNS Groups, Event List Filters, **SLA Monitors** (selected), SGT Groups.
- Main Content:** SLA Monitors page. It displays a table with columns: #, NAME, MONITORED ADDRESS, TARGET INTERFACE, and ACTIONS. A message says "There are no SLA Monitors yet. Start by creating the first SLA Monitor." A blue button labeled "CREATE SLA MONITOR" is highlighted with a red border.

سوق مترarms SLA

8. وظائف اوتوماتيكية.

يـ.سـاـسـلـاـ لـاـصـتـاـ تـامـلـعـمـ نـيـوـكـتـبـ مـقـ.

Add SLA Monitor Object



Name

Description

Monitor Address



Target Interface



IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

milliseconds

0 - 2147483647

Timeout

milliseconds

0 - 604800000

Frequency

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0 - 255

Number of Packets

0 - 100

Data Size

0 - 16384

bytes

CANCEL

OK

نئاک عاشن SLA

9. ۋەطخىلما.

قەحول ئىلە لقتىندا .5 ئاشناب تاھجى أولل تباثىلا راسىملا موقىي نأ بجى ،نئاکلا عاشندا درجمب زاھىل رز دىدەت ب ئىسېئرلا تامۇلۇملا.

The screenshot shows the 'Objects' tab selected in the top navigation bar, with the device set to 'SF3130'. The main area displays 'SLA Monitors' with one object listed:

ID	NAME	MONITORED ADDRESS	TARGET INTERFACE	ACTIONS
1	Outside_Primary_ISP	Gateway-Outside-1	outside_primary	[Edit]

ۋەش اش عاشن SLA

10. ۋەطخىلما.

5. يىجوتلا قەحول يف ضرع نېوكت دىدەت ب ھىجوتلا مىسىقىلى لقتىندا.

The screenshot shows the 'Device: SF3130' configuration page. Key details include:

- Model: Cisco Secure Firewall 3130 Threat Defense
- Software: 7.7.0-89
- VDB: 408.0
- Intrusion Rule Update: 20250605-1326
- Cloud Services: Connected | HackaTZ-2025
- High Availability: Not Configured

The device diagram shows connections to 'Inside Network' and 'ISP/WAN/Gateway'. A note indicates 'No interface named "outside"'.

Below the device diagram, several configuration sections are shown:

- Interfaces**: Management: Merged, Enabled 4 of 17. [View All Interfaces](#)
- Routing**: There are no static routes yet. [View Configuration](#)
- Updates**: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds. [View Configuration](#)
- System Settings**: Management Access, Logging Settings, DHCP Server / Relay, DDNS Service, DNS Server, Hostname, Time Services, SSL Settings. [See more](#)
- Smart License**: Registered. [View Configuration](#)
- Backup and Restore**. [View Configuration](#)
- Troubleshoot**: No files created yet. [REQUEST FILE TO BE CREATED](#)

ئىسېئرلا تامۇلۇملا قەحول

11. ۋەطخلا

يىرفوم نم لكل ئىضارىت فا ئىتابات تاراسىم 2 ئاشناب مۇق ، "تباث ھىجوت" بىيوبتلا ئەم الاع يف تباث راسىم ئاشنالا رىزلا دىچ ، دىدج تباث راسىم ئاشنالا تامىد.

The screenshot shows the Cisco Firewall Device Manager interface. The top navigation bar includes tabs for Firewall Device Manager, Monitoring, Policies, Objects, and Device: SF3130. On the right, there are icons for device status, configuration, and help, along with the user admin and role Administrator. The main content area is titled 'Device Summary' and 'Routing'. Below this, there's a search bar for 'Add Multiple Virtual Routers' and buttons for 'Commands' and 'BGP Global Settings'. The 'Static Routing' tab is active, showing sub-options for BGP, OSPF, EIGRP, and ECMP Traffic Zones. A large table header for static routes includes columns for #, NAME, INTERFACE, IP TYPE, NETWORKS, GATEWAY IP, SLA MONITOR, METRIC, and ACTIONS. A message in the center states 'There are no static routes yet. Start by creating the first static route.' Below this message is a prominent blue 'CREATE STATIC ROUTE' button, which is highlighted with a red box.

تباثلا ھىجوتلما مىسىقى

12. ۋەطخلا

يىذلا SLA ئەبلىق ئەنلا فەضىء، ئەنلا يف يىساسىلار ئەنلا ئەشنىپ مۇق ، الۋە ئەرەي خالا ئەوطخلا يف ھۆشاشنى مەت.

Add Static Route



Name _____

Route_ISP_Primary

Description

Static Route for ISP Primary

Interface

outside_primary (Ethernet1/1)

Protocol



Networks



any-ipv4

Gateway

Gateway-Outside-1

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Outside_Primary_ISP

CANCEL

OK

یس اس ال ا ISP ل تبا ثلا راس ملا

13. خطا و ة

ةرابعلا مادختساب ٰيوناچلا ISP ل ،يضرارتفا راسم عاشن او ٰريخألا ٰوطخل راركتب مق 200 ىلإ هتدايز تمت ،لاثمل اذه يف .فلتخمل سايقملا او ٰبسانمل

Add Static Route

Name: Route_ISP_Backup

Description: Static Route for ISP Backup

Interface: outside_backup (Ethernet1/2)

Protocol: IPv4 (selected)

Networks: + any-ipv4

Gateway	Metric
Gateway-Outside-2	200

SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor

CANCEL OK

یوناٹل ISP ل تباٹل راس مل

14. ةوطخلا

تاني اكل مسقى لقتنا . ناماً نقطن عاشن بجي ، نيت باشلا نيه وجوملا الاك عاشن درج مبلىع ألب دوجوملا تاني اكل رز ديجو.

Device Summary																												
Routing																												
Add Multiple Virtual Routers																												
Static Routing BGP OSPF EIGRP ECMP Traffic Zones																												
Commands BGP Global Settings																												
2 routes																												
<table border="1"><thead><tr><th>#</th><th>NAME</th><th>INTERFACE</th><th>IP TYPE</th><th>NETWORKS</th><th>GATEWAY IP</th><th>SLA MONITOR</th><th>METRIC</th><th>ACTIONS</th></tr></thead><tbody><tr><td>1</td><td>Route_ISP_Primary</td><td>outside_primary</td><td>IPv4</td><td>0.0.0.0/0</td><td>172.16.1.254</td><td>Outside_Primary_ISP</td><td>1</td><td>Edit</td></tr><tr><td>2</td><td>Route_ISP_Backup</td><td>outside_backup</td><td>IPv4</td><td>0.0.0.0/0</td><td>172.16.2.254</td><td></td><td>200</td><td>Edit</td></tr></tbody></table>		#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS	1	Route_ISP_Primary	outside_primary	IPv4	0.0.0.0/0	172.16.1.254	Outside_Primary_ISP	1	Edit	2	Route_ISP_Backup	outside_backup	IPv4	0.0.0.0/0	172.16.2.254		200	Edit
#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS																				
1	Route_ISP_Primary	outside_primary	IPv4	0.0.0.0/0	172.16.1.254	Outside_Primary_ISP	1	Edit																				
2	Route_ISP_Backup	outside_backup	IPv4	0.0.0.0/0	172.16.2.254		200	Edit																				

هؤاشن! مت يتلا قتباثلا تاراسملاء

15. ةوطخلا

مۇق مىث، رسىيەلە دۈمۈلە يىف نامالا قىطانىم رىزلا دىدەت قىرەت نع نامالا قىطانىم مىسق ئىلا لىقتىنە.
نامامۇ قىقطانىم عاشنىڭ رىزلا دىدەت قىرەت نع ۋەدىج ۋەققەنەم عاشنىڭ.

The screenshot shows the 'Object Types' section of the Firewall Device Manager interface. The 'Security Zones' option is selected and highlighted with a red box. On the right, the 'Security Zones' page is displayed, also with a red box around the 'CREATE SECURITY ZONE' button. The page includes a table header with columns: #, NAME, MODE, INTERFACES, and ACTIONS.

Object Types

- Networks
- Ports
- Security Zones**
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates
- Secret Keys
- DNS Groups

Device: SF3130

admin
Administrator

cisco SECURE

Security Zones

#	NAME	MODE	INTERFACES	ACTIONS
There are no security zones yet. Start by creating the first security zone.				

CREATE SECURITY ZONE

ةينمألا قطان ملamps

16. ۋەطخلا

ISPs تالاچىتال ئىجراخلا تاھجاولى الىك مادختساب ئىجراخلا نامالا ئققطنم عاشناب مق.

Add Security Zone

Name
outside_zone

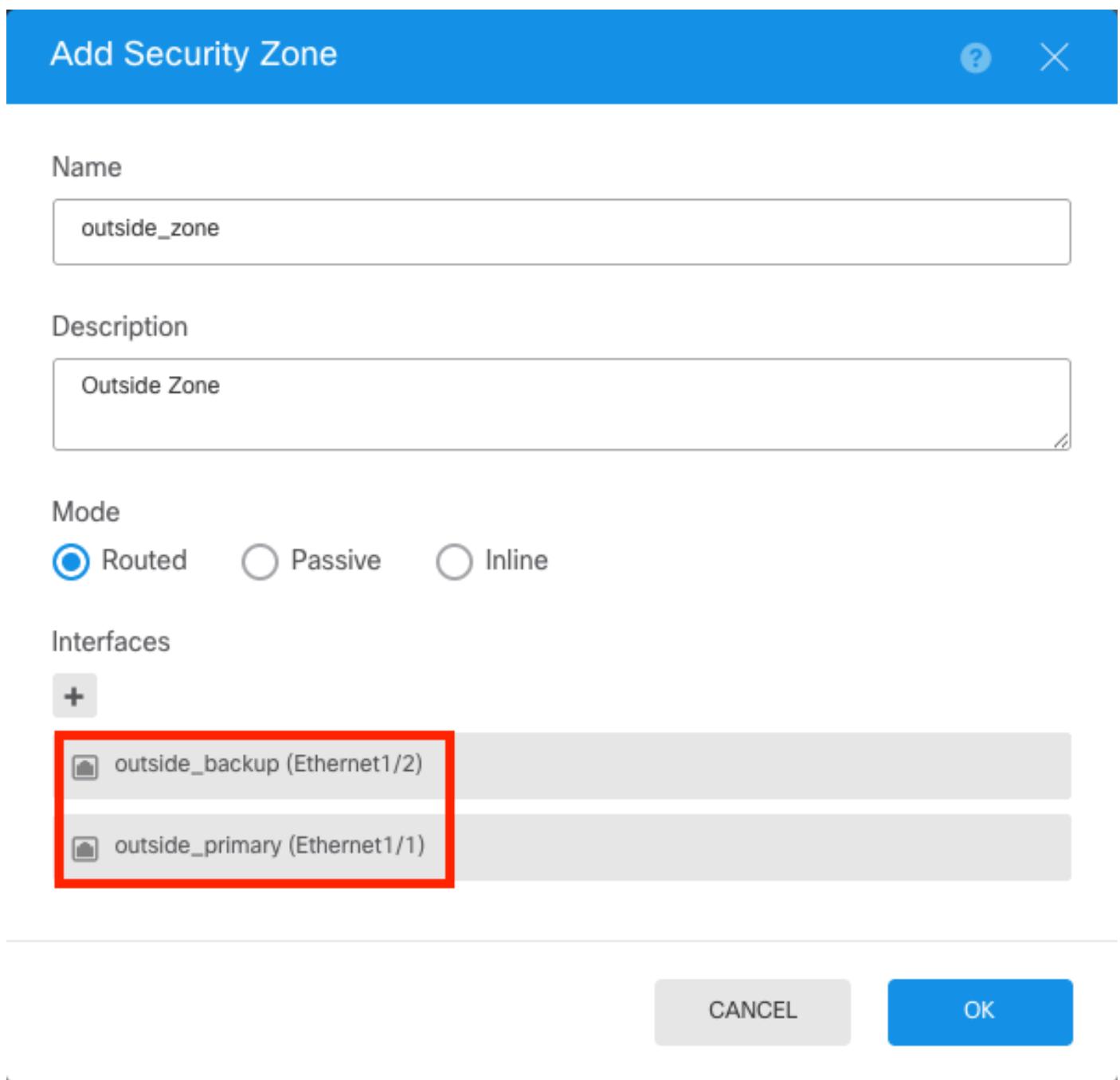
Description
Outside Zone

Mode
 Routed Passive Inline

Interfaces
+

outside_backup (Ethernet1/2)
outside_primary (Ethernet1/1)

CANCEL OK



جراخلا يف ئىنمالا ئققطنملا

17. ۋەطخلا

جەن رىزلا دىدەتلىپ تاسايىسلە مىسىقىلى لىقتىنا. NAT ئاشنى بجي، نامالا ئققطنم عاشنى دىعېلە ئىلە.

The screenshot shows the 'Objects' tab selected in the top navigation bar. The left sidebar lists various object types: Networks, Ports, Security Zones (which is the current selection), Application Filters, URLs, Geolocations, Syslog Servers, IKE Policies, IPSec Proposals, Secure Client Profiles, Identity Sources, Users, Certificates, Secret Keys, and DNS Groups. The main content area displays 'Security Zones' with 2 objects listed:

#	NAME	MODE	INTERFACES	ACTIONS
1	outside_zone	Routed	outside_backup, outside_primary	[Edit]
2	inside_zone	Routed	inside	[Edit]

At the bottom of the sidebar, there is a link to 'Event List Filters'.

نام آل قطانم عاشنإ

18. ةوطخلا

رۇز دىريختىب nat مىقىمەت، ئاشناب ئادىجى ئەدعاق ئاشناب ئەدعاق رىزلا دىريختىب nat لىقتنى.

The screenshot shows the Firewall Device Manager interface with the following details:

- Header: Firewall Device Manager, Monitoring, Policies (highlighted), Objects, Device: SF3130.
- User: admin, Administrator.
- Navigation: SSL Decryption, Identity, Security Intelligence, NAT (highlighted with a red box).
- Sub-navigation: Access Control, Intrusion.
- Search: Filter.
- Table Headers: NAME, TYPE, INTERFACES, ORIGINAL PACKET, TRANSLATED PACKET, ACTIONS.
- Table Data: There are no NAT Rules yet. Start by creating the first NAT rule.
- Action Buttons: CREATE NAT RULE (highlighted with a red box).

مسق nat

19. ةوطخلا

تاهج اولا رب ع ديدخت جاحسم نويوكتلل نوكينأ بجي، ISP لوكوتورب لشف زواحتل ئبسنلاب يساسألا ISP ب ئيساسألا ئيجراخلا ئهجاولالاصتال، الوا ئيجراخلا.

Add NAT Rule



Title

To_Internet

Create Rule for

Auto NAT

Status



Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement

Automatically placed in Auto NAT rules

Type

Dynamic

Packet Translation

Advanced Options

ORIGINAL PACKET

Source Interface

inside

Original Address

Inside

Original Port

Any

TRANSLATED PACKET

Destination Interface

outside_primary

Translated Address

Interface

Translated Port

Any

Show Diagram



CANCEL

OK

يـسـاسـاـ لـ ISP

ـ ـ وـ طـ خـ لـ اـ

ـ يـونـاـثـلـاـ ISPـ لـ اـصـتـالـ نـاـثـ natـ ،ـ نـآـلـاـ

ـ بـسـنـلـابـ ،ـ لـاـثـمـلـاـ اـذـهـ يـفـ .ـ ةـكـبـشـلـاـ سـفـنـ مـادـخـتـسـ اـنـكـمـيـ اـلـ ،ـ يـلـصـأـلـاـ نـاـوـنـعـلـلـ :ـ ظـاحـلـ

ـ اـنـيـاـكـلـاـ وـهـ يـلـصـأـلـاـ نـاـوـنـعـلـاـ نـوـكـيـ ،ـ يـونـاـثـلـاـ تـنـرـتـنـاـلـاـ تـامـدـخـ رـفـوـمـلـ any-IPv4ـ .ـ

Edit NAT Rule



Title

To_Internet_Backup

Create Rule for

Auto NAT

Status



Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement

Automatically placed in Auto NAT rules

Type

Dynamic

Packet Translation

Advanced Options

ORIGINAL PACKET

Source Interface

inside

Original Address

any-ipv4

Original Port

Any

TRANSLATED PACKET

Destination Interface

outside_backup

Translated Address

Interface

Translated Port

Any

Show Diagram



CANCEL

OK

يوناچل ا ISP

21. ووطخ ل.

رورملا ةكرحب حامسلل لوصولا يف مكحتلا ةدعاق ءاشنابجي ، NAT دعاق نم لك ءاشنادع بـ لوصولا يف مكحتلا رزلاددح . ةرداصلا

The screenshot shows the Firewall Device Manager interface with the following details:

- Header:** Firewall Device Manager, Monitoring, Policies (selected), Objects, Device: SF3130, admin Administrator, cisco SECURE.
- Breadcrumb:** SSL Decryption → Identity → Security Intelligence → NAT → Access Control (highlighted with a red box).
- Table Headers:** ORIGINAL PACKET (Source Address, Destination Address, Source Port, Destination Port) and TRANSLATED PACKET (Source Address, Destination Address, Source Port, Destination Port).
- Section:** Auto NAT Rules
- Rules:**
 - > # To_Internet DYNAMIC Inside ANY ANY Interface ANY ANY ANY ANY
 - > # To_Internet_Ba... DYNAMIC Inside outside_b... any-ipv4 ANY ANY Interface ANY ANY ANY ANY

دعاوق عاشن ام مت NAT

22. ووطخلا ۋە.

لوصو دەعاق ئاشن رىزلا دەج، لوصولاب مكەحتلا دەعاق ئاشنال.

The screenshot shows the Firewall Device Manager interface with the following details:

- Header:** Firewall Device Manager, Monitoring, Policies (selected), Objects, Device: SF3130, admin Administrator, cisco SECURE.
- Breadcrumb:** SSL Decryption → Identity → Security Intelligence → NAT → Access Control (highlighted with a red box).
- Table Headers:** SOURCE (ZONES, NETWORKS, PORTS) and DESTINATION (ZONES, NETWORKS, PORTS). Columns for APPLICATIONS, URLs, USERS, and ACTIONS are also present.
- Message:** There are no access rules yet. Start by creating the first access rule.
- Buttons:** CREATE ACCESS RULE (highlighted with a red box).
- Bottom Bar:** Default Action, Access Control (Block), and other icons.

لوصولايىف مكەحتلا مىسىق

23. ووطخلا

بۇل طەملى تاڭبىشل او قطان ملا دەج.

Add Access Rule

Order Title Action

1 To_Internet Allow

Source/Destination Applications URLs Users ¹ Intrusion Policy File policy Logging

SOURCE DESTINATION

Zones	Networks	Ports	SGT Groups	Zones	Networks	Ports	SGT Groups
Inside_zone	Inside	ANY	ANY	outside_zone	ANY	ANY	ANY

Show Diagram 



لوصول ايف مكاحتلا وداعق

24. ةوطخلا

قيرط نع تارييغتلارش نل ئەۋباتمەلاب مەق، "لۇصۇلاب مەكھىتلا ۋەدعاق" ئاشندا درەجەب ئىلعلالاب دوچومەلارش نىزىلا دىدەخت.

The screenshot shows the Firewall Device Manager interface with the following details:

- Header:** Firewall Device Manager, Monitoring, Policies (highlighted in blue), Objects, Device: SF3130.
- Top Right:** admin Administrator, Cisco SECURE.
- Breadcrumbs:** SSL Decryption → Identity → Security Intelligence → NAT → Access Control (highlighted with a red box) → Intrusion.
- Table Headers:** SOURCE (ZONES, NETWORKS, PORTS) and DESTINATION (ZONES, NETWORKS, PORTS) columns, followed by APPLICATIONS, URLs, USERS, and ACTIONS.
- Table Data:** One rule named "To_Internet" with ID 1. It has an Allow action, source zone "inside_zone", destination zone "outside_zone", and applies to the Inside network.
- Bottom Buttons:** Default Action, Access Control (highlighted with a red box), Block, and other configuration icons.

25. ةوطخلا

نآل رشن رزلا ددج مث تارييغتلانم ققحت

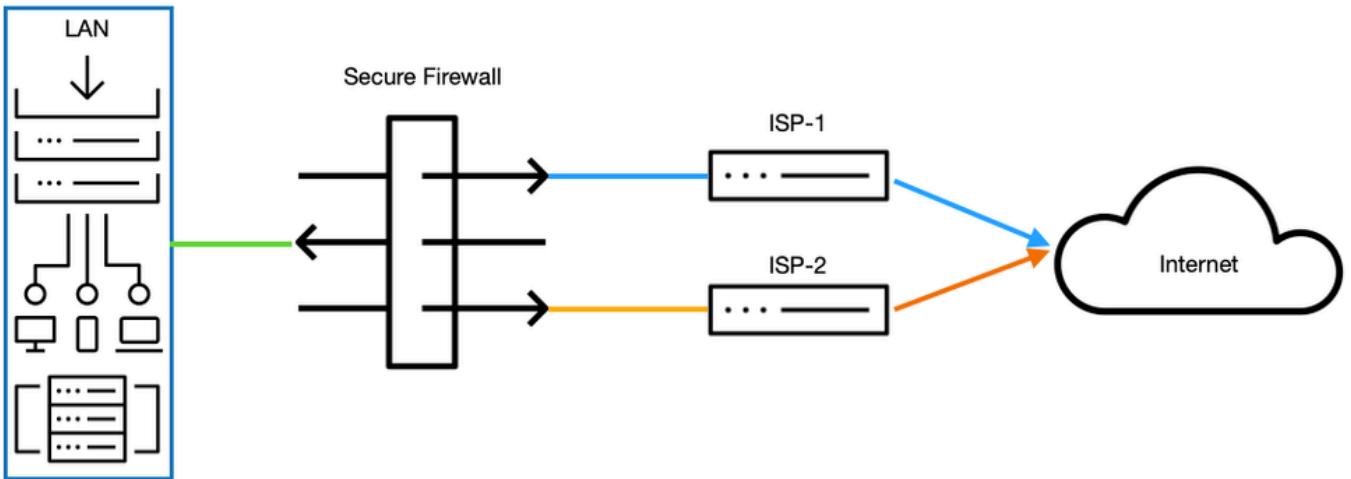
Pending Changes

Last Deployment Completed Successfully
10 Jun 2025 12:35 PM. [See Deployment History](#)

Deployed Version (10 Jun 2025 12:35 PM)	Pending Version	
+ Access Rule Added: <i>To_Internet</i>		
-	logFiles: false	
-	eventLogAction: LOG_NONE	
-	ruleId: 268435458	
-	name: To_Internet	
sourceZones:	inside_zone	
-	destinationZones:	
-	outside_zone	
sourceNetworks:	Inside	
-		
+ Security Zone Added: <i>inside_zone</i>		
-	mode: ROUTED	
-	description: Inside Zone	
-	name: inside_zone	
interfaces:	inside	
-		
+ SLA Monitor Added: <i>Outside_Primary_ISP</i>		
-	slaOperation.frequency: 60000	
-	slaOperation.threshold: 5000	
-	slaOperation.dataSize: 28	
-	slaOperation.numOfPackets: 1	
-	slaOperation.typeOfService: 0	
-	slaOperation.timeout: 5000	
-	description: Monitor for ISP Primary	
-	name: Outside_Primary_TCP	
MORE ACTIONS ▾	CANCEL	DEPLOY NOW ▾

رشنلانم ققحتلا

ةكبشلل يطيطختلارسلا



ةكبش للي طختلا مسرا

ةحصلانم ققحتلا

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
SF3130#
```

```
show ip
```

```
System IP Addresses:
```

Interface	Name	IP address	Subnet mask	Method
Ethernet1/1	outside_primary	172.16.1.1	255.255.255.0	manual

```
-----> THE PRIMARY INTERFACE OF THE ISP IS SET
```

```
Ethernet1/2 outside_backup 172.16.2.1 255.255.255.0 manual
```

```
-----> THE SECONDARY INTERFACE OF THE ISP IS SET
```

```
Ethernet1/3 inside 192.168.1.1 255.255.255.0 manual
```

```
SF3130#
```

```
show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet1/1	172.16.1.1	YES	manual	up	up

```
-----> THE INTERFACE IS UP AND RUNNING
```

```
Ethernet1/2 172.16.2.1 YES manual up up
-----> THE INTERFACE IS UP AND RUNNING
```

```
Ethernet1/3 192.168.1.1 YES manual up up
```

```
SF3130#
```

```
show route
```

```
Gateway of last resort is 172.16.1.254 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary
```

```
----> THE DEFAULT ROUTE IS CONNECTED THROUGH THE PRIMARY ISP
```

```
C 172.16.1.0 255.255.255.0 is directly connected, outside_primary
L 172.16.1.1 255.255.255.255 is directly connected, outside_primary
C 172.16.2.0 255.255.255.0 is directly connected, outside_backup
L 172.16.2.1 255.255.255.255 is directly connected, outside_backup
C 192.168.1.0 255.255.255.0 is directly connected, inside
L 192.168.1.1 255.255.255.255 is directly connected, inside
```

```
SF3130#
```

```
show run route
```

```
route outside_primary 0.0.0.0 0.0.0.0 172.16.1.254 1 track 1
route outside_backup 0.0.0.0 0.0.0.0 172.16.2.254 200
```

```
SF3130#
```

```
show sla monitor configuration
```

```
---> CHECKING THE SLA MONITOR CONFIGURATION
```

```
SA Agent, Infrastructure Engine-II
```

```
Entry number: 539523651
```

```
Owner:
```

```
Tag:
```

```
Type of operation to perform: echo
```

```
Target address: 172.16.1.254
```

```
Interface: outside_primary
```

```
Number of packets: 1
```

```
Request size (ARR data portion): 28
```

```
Operation timeout (milliseconds): 3000
```

```
Type Of Service parameters: 0x0
```

```
Verify data: No
```

```
Operation frequency (seconds): 3
```

```
Next Scheduled Start Time: Start Time already passed
```

```
Group Scheduled : FALSE
```

```
Life (seconds): Forever
```

```
Entry Ageout (seconds): never
```

```
Recurring (Starting Everyday): FALSE
```

```
Status of entry (SNMP RowStatus): Active
```

```
Enhanced History:
```

```
SF3130#
```

```
show sla monitor operational-state
```

Entry number: 739848060
Modification time: 01:24:11.029 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE

-----> THE ISP PRIMARY IS IN A HEALTHY STATE

Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

AFTERARGBSETHBNDGFSHNDGSDBFB

SF3130#

```
show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet1/1	172.16.1.1	YES	manual	down	down

-----> THE PRIMARY ISP IS DOWN

Ethernet1/2	172.16.2.1	YES	manual	up	up
Ethernet1/3	192.168.1.1	YES	manual	up	up

SF3130#

```
show route
```

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [200/0] via 172.16.2.254, outside_backup

-----> AFTER THE ISP PRIMARY FAILS, INSTANTLY THE ISP BACKUP IS FAILOVER AND IS INSTALL IN THE ROUTER

C	172.16.2.0	255.255.255.0	is directly connected, outside_backup
L	172.16.2.1	255.255.255.255	is directly connected, outside_backup
C	192.168.1.0	255.255.255.0	is directly connected, inside
L	192.168.1.1	255.255.255.255	is directly connected, inside

SF3130#

```
show sla monitor operational-state
```

Entry number: 739848060
Modification time: 01:24:11.140 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever

Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE

-----> AFTER THE DOWNTIME OF THE PRIMARY ISP THE TIMEOUT IS FLAGGED

Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

SF3130#

show route

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary

-----> AFTER A FEW SECONDS ONCE THE PRIMARY INTERFACE IS BACK THE DEFAULT ROUTE INSTALLS AGAIN IN

C 172.16.1.0 255.255.255.0 is directly connected, outside_primary
L 172.16.1.1 255.255.255.255 is directly connected, outside_primary
C 172.16.2.0 255.255.255.0 is directly connected, outside_backup
L 172.16.2.1 255.255.255.255 is directly connected, outside_backup
C 192.168.1.0 255.255.255.0 is directly connected, inside
L 192.168.1.1 255.255.255.255 is directly connected, inside

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).