

# ماظن ASR1002 مع IPSec و NetFlow و NBAR

تایوتیم

ةمدقمل

ڈیس اسٹام ول ۴

و NetFlow و NBAR ماظن دییقت: ۀلکشملا ع ام ASR1002 و IPSec

نیوکل

تاظحالم

لحل

ةمدقملا

نیوکت عم ASR1002 يس اس الـ ماظنـا ىلـع ئـيـجـاتـنـا عـم ئـلـكـشـمـلـا دـنـتـسـمـلـا اـذـهـ حـضـوـيـ  
هـجـومـلـا ىـلـع IPSec ـقـيـزـمـ مـادـخـتـسـابـ (AVC) مـكـحـتـلـاـوـ قـيـبـطـتـلـاـ ئـيـفـرـ ئـيـنـاـكـمـاـ.

ةيسي اسأ تام ولع

ةكحـل ئـينـاـثـلـا يـف تـبـاجـيـج 10 ئـعـرـسـبـ ئـجـلـاعـمـ ئـعـسـ ASR10002 رـفـوتـ، CCO قـئـاـشـولـ اـقـفـوـ رـيـذـحـتـ كـانـهـ نـكـلـوـ وـ IPSecـ ئـزـيمـ نـيـكـمـتـ عـمـ ئـيـنـاـثـلـا يـف تـبـاجـيـج 4، ئـيـدـاعـلـا تـانـايـبـلـا رـورـمـ نـمـ رـيـثـكـلـا كـلـهـتـسـتـ نـاتـزـيـمـ اـمـهـ NetFlowـ وـ NBARـ ASR1002ـ. ئـصـنـمـ ئـلـعـ جـرـخـلـابـ طـبـتـرـمـ نـامـأـ ئـلـوـمـحـ ئـقـاطـبـ لـيـصـوـتـ ئـيـنـاـكـمـاـ نـمـ لـلـقـتـ مـثـ نـمـوـ (QFP)ـ مـكـلـاـ قـفـدـتـ جـلـاعـمـ نـمـ درـاوـمـلـا عـمـ يـلـامـجـالـا مـاظـنـلـا جـارـخـاـ لـيـلـقـتـ يـلـاتـلـابـ وـ رـورـمـلـا ئـكـحـنـمـ دـيـزـمـلـا ئـجـلـاعـمـلـ (ESP)ـ نـيـمـضـتـلـا يـلـكـلـا جـاتـنـإـلـا ضـفـخـنـيـ نـأـ نـكـمـيـ، IPSecـ لـوـكـوـتـوـرـبـ عـمـ يـسـيـطـانـغـمـوـرـهـكـلـا قـفـاـوتـلـا ئـيـيـهـتـ رـورـمـلـا ئـكـحـ يـفـ ئـرـيـبـكـ ئـرـاسـخـ هـجـاـويـ نـأـ نـكـمـيـ وـ ئـدـشـبـ لـمـعـلـا ئـصـنـمـلـ.

لکشم ملا ماظن دییقت: ASR1002 عム IPsec و NetFlow و NBAR

رابتخا عاجا متى و رفوملا عم يددرتللا قاطنلا ئيقرت دنع رمألا ئداب يف ئلكلشملا ئظحالم مت  
مث ، امامت ديج وحن ئيلع راس امم ، تياب 1000 مجحوب ئمزح لاسرا مت ئيادبلا يف . يددرتللا قاطنلا  
نادقف ابييرقت او ئظحال دق مهناف كلد دعب و تياب 512 مجحوب مزح مادختساب رابتخالا عاجا مت  
؛ ذه ربتخملا رابتخا ايجولوبط ئيلا عجرا . 80% ئبسنب رورملما ئكرح



تازىملا ھ ذه ليغشتب مق:

- DMVPN ربع IPSec
- Netflow
- NBAR (مدخل ادوج ئاسايىس ۋ قباطم نايىب نم عزجك)

## نېوكتلار

```

crypto isakmp policy 1
encr 3des
group 2
crypto isakmp policy 2
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 0.0.0.0
crypto ipsec security-association replay disable
crypto ipsec transform-set remoteoffice-vpn esp-3des esp-sha-hmac
mode tunnel
crypto ipsec transform-set IPTerm-TransSet esp-3des esp-sha-hmac
mode tunnel
crypto ipsec profile IPTerminals-VPN
set transform-set IPTerm-TransSet
crypto ipsec profile vpn-dmvpn
set transform-set remoteoffice-vpn
!
<snip>
class-map match-any Test
match ip precedence 2
match ip dscp af21
match ip dscp af22
match ip dscp af23
match access-group name test1
match protocol ftp
match protocol secure-ftp
!
policy-map test
<snip>
!
interface Tunnel0
bandwidth 512000
ip vrf forwarding CorpnetVPN
ip address 10.1.1.1 255.255.255.0
no ip redirects
ip mtu 1350

```

```

ip flow ingress
ip nhrp authentication ldcBb
ip nhrp map multicast dynamic
ip nhrp network-id 1000
ip nhrp holdtime 600
ip nhrp shortcut
ip nhrp redirect
ip virtual-reassembly max-reassemblies 256
ip tcp adjust-mss 1310
ip ospf network point-to-multipoint
ip ospf hello-interval 3
ip ospf prefix-suppression
load-interval 30
qos pre-classify
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 1234
tunnel protection ipsec profile vpn-dmvpn
!
int gi 0/1/0
bandwidth 400000
ip address 12.12.12.1 255.255.255.252
load-interval 30
negotiation auto
ip flow ingress
service-policy output PM-1DC-AGGREGATE
!

```

نم تانايبل رورم ڈکرچ عاشن م. ASR1k. Dynamic Multipoint VPN (DMVPN) تاهجوم نيب ڈي نا ثل يف ڈمنز 50000 لکل تياب 512 غلبی ڈمنز مچحب DMVPN ڈب اس ربع IXIA ڈل IXIA ڈل IXIA نم (EF) عيرسل ڈيجوتلا ڈادا رورم ڈکرچل رخا ق فدت نيوكت مت

ييف ڈحفص 30000 ڈل لصي امل نيرودلا الک يف رورمل ڈکرچ نادقف ان ظحال، هالعأ ڈفدل ا عم ڈي نا ثل.

## تاظح الام

ڈئف يف دهاشت ڈريثك ضافخنا تالاح الوجتنل اضافخنا تالاح يف ڈادي زكانه نكت مل ڈمدخل جھنل ڈي ضارت فالا ڈئفل نم الـ ڈرخـ ڈـ اـ ڈـ فـ وـ اـ.

تـ ايـ ڈـ اـ صـ حـ الـ اـ تـ طـ قـ سـ اـ بـ يـ فـ طـ وـ بـ تـ الـ اـ حـ تـ دـ جـ وـ عـ يـ رـ سـ لـ كـ شـ بـ دـ يـ اـ زـ تـ تـ نـ اـ كـ لـ تـ طـ وـ قـ سـ لـ اـ تـ الـ اـ حـ نـ أـ تـ ظـ حـ الـ وـ ڈـ طـ شـ نـ لـ اـ.

```
RTR-1#show platform hardware qfp active statistics drop
```

```
-----
Global Drop Stats Packets Octets
-----
IpsecInput 300010 175636790
IpsecOutput 45739945 23690171340
TailDrop 552830109 326169749399
```

```
RTR-1#
```

```
RTR-1#show platform hardware qfp active statistics drop
```

```
-----
Global Drop Stats Packets Octets
-----
```

```
IpsecInput 307182 179835230  
IpsecOutput 46883064 24282257670  
TailDrop 552830109 326169749399
```

RTR-1#

رمألا مادختساب IPSec ل طاقس ا تاييلمع نم ديزملانم ققحتلا ماتhardware qfp IPsec

```
RTR-1#show platform hardware qfp active feature ipsec data drops
```

---

-----

Drop Type Name Packets

[View Details](#) | [Edit](#) | [Delete](#)

28 IN\_PSTATE\_CHUNK\_ALLOC\_FAIL 357317

54 OUT\_PSTATE\_CHUNK\_ALLOC\_FAIL 51497757

66 N2\_GEN\_NOTIFY\_SOFT\_EXPIRY 4023610

RTR-1#

دادع عم قباطتی **IN\_PSTATE\_CHUNK\_ALLOC\_FAIL** دادع طاقس إلا دادع نأ ظحالم مت **IPsecInput** دادع عم قباطتی يذلا **IPsecOutput** دادع قباطتی و **QFP** طاقس إتايلمع يف **OUT\_PSTATE\_CHUNK\_ALLOC\_FAILED**.

#لخ ۋېجىم ربلا يلى بىچ او رادصا اذه تىيار CSCuf25027 .

لحن

ىلإ دنتسملا قيبطتلارا ىلع فرعتلا "زيم لمي طمعت و هـ ئـلـكـشـمـلـاـ هـذـهـلـ لـيـدـبـلـاـ لـحـلـاـ لـوـصـحـلـاوـتـازـيـمـلـاـ عـيـمـجـ لـيـغـشـتـ يـفـ بـغـرـتـ تـنـكـ اـذـاـ .5ـ جـوـمـلـاـ ىـلـعـ "NetFlow وـ" (NBAR) ئـكـبـشـلـاـ وأـXـ ASR1002ـ إـلـاـ ئـيـقـرـتـلـاـ يـفـ لـضـفـأـلـاـ رـايـخـلـاـ لـثـمـتـيـفـ ،ـلـضـفـأـقـجـاعـمـ ـعـسـ ىـلـعـ ESP-100ـ مـادـخـتـسـابـ.

## 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).