

ةباحسلا ةرابعل يبهدلا نيوكتلا نيوكت

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتلا](#)

[تابلطتلا](#)

[ةمدختسلا تانوكملا](#)

[تاسايسلل يحصلا رجحلا](#)

[Cloud Gateway Gold نيوكت](#)

[يساسألا نيوكتلا](#)

[ةينمألا تامدخلا](#)

[ماظنلا ةرادا](#)

[\(ةيرايتخا\) ةيفاضا ةئيهت](#)

[\(CLI\) رماوأل رطس ةهجاو يوتسم تاريغت](#)

[\(HAT\) فيضملا لول لوصولا لودج > ديربلا تاسايس\) فيضملا لول لوصولا لودج](#)

[\(ةيضارتفالاجهنلا تاملعم\) ديربلا قفدت جهن](#)

[دراولا ديربلا جهن](#)

[رداصللا ديربلا جهن](#)

[يرخأ تادادعا](#)

[\(سيميوقلا > ديربلا تاسايس\) سيميوقلا](#)

[\(ةهجولا مكحت رصانع > ديربلا تاسايس\) ةهجولا مكحت رصانع](#)

[يوتحمللا ةيفصت لماع](#)

[ةدراولا يوتحمللا ةيفصت لماع](#)

[ةرداصللا يوتحمللا ةيفصت لماع](#)

[Cisco Live](#)

[ةيفاضا تامولعم](#)

[Cisco نم ةنمأل ينورتكلاللا ديربلا ةرابع قيثوت](#)

[ةنمأل ينورتكلاللا ديربلا ةباحس ةرابع قيثوت](#)

[Cisco نم بيولا ريدمو نمأل ينورتكلاللا ديربلا قيثوت](#)

[Cisco نم نمأل اجت نملا قيثوت](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ديربلا ةباحس ةباوبل رفوتملا يبهدلا نيوكتلل اقمعتم اليلحت دنتسملا اذه فصلي نمأل ينورتكلاللا ديربلا ةباحس ءالمعل يبهدلا نيوكتلل دعي. Cisco نم ةنمأل ينورتكلاللا و Cisco Secure Email و ةباحسلا ةرابع نم لكل موي نودب نيوكتو ةسرامم لصفأ وه Cisco نم لك Cisco نم ةنمأل ينورتكلاللا ديربلا ةباحس رشن تايلمع مدختست. Web Manager نم ءانجأ موقت. لقالا يلع بيولا ريدمو (1) دجاو ينورتكلاللا ديربلا ةباحسلا (تارابع) ةرابع ديربلا يلع دوجوملا لزعلا مادختسا لول نيولوؤسملا هيچوتب تاسرامملا لصفأ نيوكتللا ةيزكرملا ةراداللا ضارغأل بيولا ريدمو ينورتكلاللا

ةيساس الابلطتم

تابلطتم

عوضوم اذه فرعت تنأ نأ صوي cisco:

- ةرادو مدختسملا ةهجاو نم الك، ةباحسلا ةرابع وأ Cisco نم نمآلا ينورتكلإلا ديربلا ةرابع رم اوألا رطس ةهجاو
- مدختسملا ةهجاو يوتسم Cisco، نم بيولا ريومو نمآلا ينورتكلإلا ديربلا ةرادو
- عجار عاجر؛ CLI لوصو بلط Cisco نم نمآلا ينورتكلإلا ديربلا ةباحس ءالمعل نكمي: [\(CLI\) رماوألا رطس ةهجاو لوصولا](#)

ةمدختسملا تانوكملا

لض فأ تايصوتو يبهذلا نيوكتللا نم ةدمتسم دنتسملا اذه في ةدراولا تامولعمل اهيلوؤسمو Cisco نم نمآلا ينورتكلإلا ديربلا ةباحس ءالمعل تاسرامملا.

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجالا نم دنتسملا اذه في ةدراولا تامولعمل ءاشنإ مت تناك اذإ. (يضارتفا) حوسمم نيوكتب دنتسملا اذه في ةمدختسملا ةزهجالا عيمج تادب رما يال لمتمحمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تبش.

ةلصللا تاذا تاجتنملا

ىلع اضيا دنتسملا اذه قبطني:

- Cisco نم ةنمآلا ينورتكلإلا ديربلا ةرابعل ةيضارتفاللا ةزهجالا وأ ةيلحمللا ةزهجالا
- Cisco نم نمآلا بيولا ريومو ةيلحمللا ةيضارتفاللا ةزهجالا او ةزهجالا

تاسايسلل يحيصللا رجحلا

ةباحس ءالمعل بيولا ريومو ينورتكلإلا ديربلا لىل ةنايصللاو رجحلا تايلمع نيوكت متي ةرادو ينورتكلإلا كدير لىل لوخدلا ليحست يجرى Cisco. نم نمآلا ينورتكلإلا ديربلا يحيصللا رجحلا ضرعل بيولا:

- ACCOUNT_TAKEOVER
- لاجتناللا داضم
- BLOCK_ATTACHMENTS
- عنملا ةمئاق
- Dkim_Fail
- لبميس_كرام
- صفر_كرام
- فيزمللا ينورتكلإلا ديربلا

- ىوتحمل بسانم ريغ
- وركام
- Open_Relay
- ةصاخلا بحسلا قوقح_تاناي ب
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_Malicious

نيوكت Cloud Gateway Gold

لضفا ىلى اذانتسا (تانويكتلا) نيوكتلا في تاريغت يا ةعجارم بجي: ريذحت في نيوكتلا تاريغت ذي فننت لبق اهمهفو دننسملا اذه في حضوم وه امك تاسرامملا ني عمل ةمدخلال ري دم وا Cisco CX سندنهم ةراشتسا ي جري. كب ةصاخلا جاتنال ةئيب (DSM) نيوكتلا تاريغت لبق باسحلا قيرف وا

يساسالا نيوكتلا

(RAT) ملتسملا لوصو لودج > ديربلا جهن

ددحي. ماعلا يغصملا لبق نم مهلوبق متي نيذلا نيملتسملا "ملتسملا لوصو لودج" ددحي ةفاضلا RAT ةعجارم عاجرلا. هضفر وا هولوبق متيس ناك اذا امو لقالا ىلع ناوئعلا لودجلا ةعاجلا بسح اهترادوا تالاجملا.

SMTP تاراسم > ةكبش

[يذلا Office365 ل ديذلا ليثملا](#) ةعجارم عاجرلاف، Microsoft 365 يه SMTP راسم ةهجو تناك اذا اقحالا ىرخا ةرم ةلواجملا ي جري. لوغشم Server 4.7.500 ىلع يوتحي

ةينمالا تامدخال

Cisco نم نم آلا ي نورتكلالال ديربلا ةباحس ءالمع عي مجل ةجرمدلا تامدخال نيوكت متي ةمدقملا ميقلاب

IronPort Anti-Spam (IPAS)

- اقلطم 2M ل يئوئضلا حسملا مدعو امئاد هنيوكتو 1M ل يئوئضلا حسملا نيكمت
- ةيناث 60: ةدحاو ةلاس رصح ةلهم
- URL ةيفصت

- ةعمسلا او URL في نصت ةيفصت لم اوع نيكمت

- "bypass_urls." م س ا ب ه ن ي و ك ت و URL ل AllowList ء ا ش ن ا ب م ق (ي ر ا ي ت خ |)
- ب ي و ل ا ل ع ا ف ت ب ق ع ت ن ي ك م ت
- URL ن ي و ا ن ع د د ع ل ي ص ق ا ل ا د ح ل ا ي ن ا ت 15 URL ن ا و ن ع ن ع ث ح ب ل ا ة ل ه م : ة م د ق ت م ل ا ت ا د ا د ع ا ل ا ي ف HREF و URL ص ن ة ب ا ت ك ة د ا ع ا 400 : ق ف ر م ل ا و ي س ا س ا ل ا ص ن ل ا ي ف ا ه ص ح ف م ت ي ت ل ل ن ك م م URL ل ي ج س ت ا ل : ة ل ا س ر ل ا
- ج ا ل ع و URL ل ي ع ج ر ل ا م ك ح ل ا ر ف و ت ي ، [AsyncOS 14.2 ل Cloud Gateway](#) ن م ا ر ا ب ت ع ا (ي ر ا ي ت خ |) [د ي ر ب ل ا ة ر ا ب ع ل URL ة ي ف ص ت ن ي و ك ت ب م ق و](#) ة م د ق م ل ا ر ا د ص ا ل ا ت ا ط ح ا ل م ع ج ا ر ، URL [ق ب ا ح س ل ا ة ب ا و ب و ن م ا ل ا ي ن و ر ت ك ل ل ا ل ا](#)

Graymail فاشتك

- م 2 ل ي ء و ض ل ا ح س م ل ا م د ع و ه ن ي و ك ت و م 1 ل م ء ا د ل ا ي ء و ض ل ا ح س م ل ا ن ي ك م ت
- ة ي ن ا ت 60 : ة د ح ا و ة ل ا س ر ر ص ح ف ة ل ه م

ي ش ف ت ل ا ة ي ف ص ت ل م ا و ع

- ة ف ي ك ت م ل ا د ع ا و ق ل ا ن ي ك م ت
- م 2 : ا ه ص ح ف ب و ل ط م ل ا ة ل ا س ر ل ا م ج ح ل ي ص ق ا ل ا د ح ل ا
- ب ي و ل ا ل ع ا ف ت ب ق ع ت ن ي ك م ت

ه ل ي ل ح ت و ف ل م ل ا ة ع م س > ة ر ا ض ل ا ج م ا ر ب ل ا ن م ة م د ق ت م ل ا ة ي ا م ح ل ا

- ف ل م ل ا ة ع م س ن ي ك م ت
- ت ا ف ل م ل ا ع ا و ن ا ة ع ج ا ر م ل " ة ي م و م ع ل ا ت ا د ا د ع ا ل ا " ة ع ج ا ر م ا ج ر ل ا ت ا ف ل م ل ا ل ي ل ح ت ن ي ك م ت ت ا ف ل م ل ا ل ي ل ح ت ل

ل ئ ا س ر ل ا ب ق ع ت

- (ا ب و ل ط م ك ل ذ ن ا ك ا ذ ا) ض و ف ر م ل ا ل ا ص ت ا ل ا ل ي ج س ت ن ي ك م ت

م ا ط ن ل ا ة ر ا د ا

(ن و م د خ ت س م ل ا > م ا ط ن ل ا ة ر ا د ا) ن و م د خ ت س م ل ا

- ة ر ا ب ع ت ا د ا د ع ا و ي ل ح م ل ا م د خ ت س م ل ا ب ا س ح ب ة ط ب ت ر م ل ا ر و ر م ل ا ة ر ا ب ع ت ا س ا ي س ة ع ج ا ر م ر ك ذ ت ا ه ن ي ي ع ت و ر و ر م ل ا
- (LDAP) ل ي ل د ل ل ل و ص و ل ل ف ي ف خ ل ل و ك و ت و ر ب ل ا ن ي ك م ت و ن ي و ك ت ب م ق ، ن ك م ا ن ا (LDAP > م ا ط ن ل ا ة ر ا د ا) ة ق د ا ص م ل ل

(ت ا ك ا ر ت ش ا ل ا ل ي ج س ت > م ا ط ن ل ا ة ر ا د ا) ت ا ك ا ر ت ش ا ل ا ل ي ج س ت

- ل ي م ع ت ا ل ج س ن ي و ك ت ل ا ت ا ط و ف ح م ت ا ل ج س : ن ي ك م ت و ء ا ش ن ا ب م ق ، ن ي و ك ت ل ا م د ع ة ل ا ح ي ف URL ة ع م س
- ، ل ا س و و ر ل ا ة ف ا ض ا و ت ا د ا د ع ا ل ا ر ي ر ح ت ب م ق ، " ل ج س ل ا ت ا ك ا ر ت ش ا ل ا ة ي م و م ع ل ا ت ا د ا د ع ا ل ا " ي ف ل س ر م ل ا ، ل ا د ر ل ا ، ن م

(ة ي ر ا ي ت خ |) ة ي ف ا ض ا ة ي ه ت

ر ط ن ل ل ا و ض ا ر ع ت س ا ل ل ة ي ف ا ض ا ت ا م د خ

LDAP > م ا ط ن ل ا ة ر ا د ا

- نكومي SSL عم LDAP يصوي cisco، LDAP تنأ لكشي نا
عافد URL

- [عباحسلا عباوبو نمآلا ينورتكلال ديربلا قرابعل URL ةيفصت نيوكت](#) ةعجارم عاجرلا
URL نع عافدلل ثدحالل نيوكتلا تاسرامم لضفأ لعل لوصحلل
- [URL Defense Guide ناونع](#) عجار عاجر، URL ناونع عافد يف قمعب اضيأ Cisco لخادتت
- URL ناونع نع عافدلا ليلد يف ةدراولا ةلثمألا ضعب دنتسمل اذه يف تجردأ امك

SPF

- كذل. ةباحسلا قرابع لىل ايجراخ (SPF) لسرمل جهن لمع راطال DNS تالجس عاشنإ متي،
يف DMARK و DKIM و SPF تاسرامم لضفأ عاشنإب عالمعل عيمج ةدشب Cisco يصوت
لعل لوصحلل [تاسرامملا لضفأو SPF نيوكت](#) ةعجارم عاجرلا. مهب ةصاخلا نامألا ةيعضو
SPF ةحص نم ققحتلا لوح تامولعمل نم ديزم
- عيمجل وركام رشن متي، Cisco نم نمآلا ينورتكلال ديربلا ةباحس عالمعل ةبسنلاب
ةزهجال عيمج ةفاضل ليهستل صيصختل فيضم مسال لكل ةباحسلا (تارابع) قرابع
ةفيضملا
- ادوجوم ناك اذا، لىلحال (SPF) DNS TXT لجس نمض -all و ~all لبق اذه عض:

exists:%{i}.spf.<allocation>.iphmx.com

SPF تالجس ةحص نم ققحت. لكل- و لكل~ب امإ يهتني SPF لجس نا نم دكأت: **ةظالم**
!تاريغت يا دعبو لبق كب ةصاخلا تالاجملل

- SPF لوح ديزملا لعل لوصحلل اهب يصوملا تاودالو تامولعمل
[SPF - لك SPF - لجس ةغايص لودج \(dmarcian.com\) يناجم SPF ثحب - لجس ققدم](#)
[dmarcian.com](#)

SPF لوكوتوربل ةيفاضل ةلثمأ

- "ةباحسلا عباوب" نم ينورتكلال ديرب لئاسر يقلتت تنك اذا وه SPF لعل زاتم لاثم
مادختسإ كنكمي. ىرخأ ديرب مداوخ نم ةرداص ينورتكلال ديرب لئاسر لسرتو كب ةصاخلا
ديربلا يف فيضم ديدحتل "a:" ةيلأ

v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~all

- كنكمي، طقف "ةباحسلا عباوب" لالخنم ةرداص ينورتكلال ديرب لئاسر لاسراب تمق اذا
مادختسإ

v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~all

- IP ناونع قاطن و IP ناونع "ip6:" و "ip4:" ةيلأ دحت، لاثملا اذه يف

v=spf1 exists:%{i}.spf.<allocation>.iphmx.com ip4:192.168.0.1/16 ~all

رم اوأال رطس ةهجاو ىوتسم تاريغي غت (CLI)

ينورتك لإلإل دي ربال ةباحس ءالم عمل نكمي ، ةيساس أال تابلطتم لإ يف ةراش لإلإل تمتم امك
(CLI) [رم اوأال رطس ةهجاو لوصو](#) ةعجارم ءا ربال ؛ CLI لوصو بلط Cisco نم نأال

ةي وهال لإحتنال داضم حشرم

- لإحتنال ءحفاكمل تاسرامم لإلإل [ءعجارم نم دكأتلإل ىجري](#)
- دي ربال ءفص لإحتنال ع نمل نيوكتل تاسرامم لإلإل ءفأو ءقيمع ءلثمأ لإلإل اذهل كل مدقي
ينورتك لإلإل

سأر ءفصت لماع ءفاضا

- هنكمت و [addHeaders](#) [لئاسر ءفصت لماع](#) ءباتك ىجري ، طقف (CLI) رم اوأال رطس ةهجاو :

```
addHeaders: if (sendergroup != "RELAYLIST")
{
  insert-header("X-IronPort-RemoteIP", "$RemoteIP");
  insert-header("X-IronPort-MID", "$MID");
  insert-header("X-IronPort-Reputation", "$Reputation");
  insert-header("X-IronPort-Listener", "$RecvListener");
  insert-header("X-IronPort-SenderGroup", "$Group");
  insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

فيضمم لإلإل لوصول لودج > دي ربال تاسايس) فيضمم لإلإل لوصول لودج (HAT))

ةي فاضال لإلإل نيلسررم تاعومجم > HAT ىل ع ءماع ءرطن

- ىل ع ءضو - Bypass_SBRs [لئاسر لإلإل ءلإل ءلإل لسررم ءعومجم ءاشنإل](#) : ESA مدختسم لإلإل
حشرم نم ءج - MY_TRUSTED_SPOOF_HOSTS ءعومسم لإلإل ىطختت ىتلإل رداصم لإلإل
ةي رابج لإلإل TLS تالاصتال - TLS_REQUIRED لإلإل
اقبسم ءدحم لإلإل SuspectedList ىل لسررم ءعومجم ىف

- لإلإل ىل ع SBRs تامال ع " نيكمت [فيضمم لإلإل](#) : لسررم لإلإل نم ققحتلإل : ESA مدختسم لإلإل
لش ف ب بسب فيضمم لإلإل PTR لجم ن ع ثحب لإلإل لىصوت لش ف نيكمت (ىراىتخا) . " ءيش
تقوم لإلإل DNS .

جذومن Aggressive HAT

- Block_Refuse [-10.0 ىل -9.0] ءسايس
- BLOCKED_REJECT [-2.0 ىل -9.0] : [-BLOCKLIST_REJECT] جهن
- دمأ : " ءيش ال " جهنل SBRs تامال ع و 0.0 ىل -2.0] نىهبتشم لإلإل ءمئاق
- ءلوبقم : لوبق لإلإل ءلباق لإلإل [0.0 ىل 10.0] ءسايس

لكشب اهنىوكت مت ىتلإل (MFP) دي ربال قفدت تاسايس HAT ءلثمأال رهظت : ءظالم

ديربال بي باناً طخ مهف" ىل اوجرلا ىجرى، MFP ل ةلماك تامولعم ىل لوصحلل. ىفاضاً بسانملا رادصال اىل لوصحلل [مدختسملال لىلد](#) ىف "ىقلىتملا/دراولا > ىنورتكلال اهرشنب تمق ىتل Cisco نم ةنمالا ىنورتكلال اىل ديربال ةباوبل AsyncOS نم

لاثم اذه:

Sender Groups (Listener: IncomingMail)															
Add Sender Group...		SenderBase™ Reputation Score (?)					External Threat Feed Sources Applied	Mail Flow Policy	Delete						
Order	Sender Group	-10	-8	-6	-4	-2	0	2	4	6	8	+10			
1	SMA												None applied	RELAYED	
2	CISCO_MONITORING												None applied	ACCEPTED	
3	RELAYLIST												None applied	RELAYED	
4	TLS_REQUIRED												None applied	TLS_REQUIRED	
5	MY_TRUSTED_SPOOF_HOSTS												None applied	ACCEPTED	
6	BYPASS_SBRS_SPAM												None applied	ACCEPTED_NOSPAM	
7	BYPASS_SBRS												None applied	ACCEPTED	
8	BLOCKLIST_REFUSE	=====											None applied	BLOCKED_REFUSE	
9	BLOCKLIST_REJECT	=====											None applied	BLOCKED_REJECT	
10	SUSPECTLIST					=====							None applied	THROTTLED	
11	FREEMAIL												None applied	THROTTLED	
12	ACCEPTLIST							=====					None applied	ACCEPTED	
	ALL												None applied	ACCEPTED	

ةيضارتفالال جهنلا تاملعم) ديربال قفدت جهن

ةيضارتفالال جهنلا تاددحم

نيمأتلا تادادع

- لصفم ىل ل (TLS) لقنلا ةقبط ناماً طبض
- لسررملا جهن لمع راطل نىكمت (SPF)
- DomainKeys (DKIM) ل فرعملال ديربال نىكمت
- قفاوتلا نم ققحتلا او ريراقتلا دادع او لاجملا ىل ةدنتسملا لئاسرلا ةقداصم نىكمت ةمجملا تاظحالملا ريراقت لاسراو (DMARK)

لوح تامولعملال نم ديزمل. نىوكتلل طبضلال نم ديزم ىل DMARK جاتحي: ةظالم ىف "DMARK نم ققحتلا > ىنورتكلال اىل ديربال ةقداصم" ىل اوجرلا ىجرى، DMARK، ديربال ةباوبل AsyncOS نم بسانملا رادصال اىل لوصحلل [مدختسملال لىلد](#) اهرشنب تمق ىتل Cisco نم ةنمالا ىنورتكلال اىل

دراول دي ربلل جهن

ل لثامم يضا رتفالال جهنلل نيوكت مت

يئاوشعال دي ربلل ةحفاكم

- ةدايز لىل لىجستللا لىدعت ي دوؤي دق). ةيضا رتفالال دودحلال دنع دودحلال كرت عم، نكمم (ةئطاخال تايباچيإلا).

تاسوري فال ةحفاكم

- "X سار ني مضا" رايخالال ةناخ ني كمت مت طقف تاسوري فال صحفا: لئاسرلل صحفا
- مق، سوري فال ةباصملا لئاسرللاو ايئوض اءحسم نكمي ال يتللا لئاسرلل ةبسنلاب ال لىل ةيصلأالا لئاسرلل ةفشرا ني يعتب

AMP

- تاراخي مدختسا، لئاسرللا ءاطخأ لىل ءيئوض اءحسم نكمي ال يتللا تاءارجلال ةبسنلاب .ححص: ءميقل، X-TG-MSGERROR، ءلاسرللا لىل صصخم سار ءفاضا و ءمدقتم
- تاراخي مدختسا، لءءملا دح لىل ءيئوض اءحسم نكمي ال يتللا تاءارجلال ةبسنلاب .ححص: ءميقل، X-TG-LIMIT، ءلاسرللا لىل صصخم سار ءفاضا و ءمدقتم
- لىل قبطملا ءارجلال مدختسا، فلملا لىلحت قىلعت مت يتللا لئاسرلل ةبسنلاب "لزع": ءلاسرللا

ل يمي ارغ

- صن ءفاضا لءاءال عم، (ءءملا، يءامءالال، قىوسءالال) رارق لءل صءفال ني كمت متي مي لست وه ءارجلال ءوضوملا لىل
- صصخم سار ءفاضا و ءمدقتم تاراخي مدختسا، ماها ل ريغ دي ربلل لىل ءارجلال ءاخءال .ححص: ءميقل، X-Bulk: (ي رايءال)

ىوتءملا ءي فست لم اوع

- و URL_REWRITE_SUSPICIOUS و URL_QUARANTINE_MALICIOUS و Enabled ديءت مت و URL_INAPPROPRIATE و DKIM_FAILURE و SPF_HARDFAIL و Executive_SPOOF و Domain_SPOOF و SDR و TG_RATE_LIMIT
- لىلءلا اءه يءاقءال هءه ىوتءملا ءي فست لم اوع رىفوت متي

ي شءفال ءي فست لم اوع

- ناك اءا. كء ءصاخال نامألا تابلطتم عم في كءلالا لىءري؛ 3 وه يضا رتفالال ديءءلالا ىوتسم "ءابولال لزع" لىل ءلاسرلل لقتنت، هءواءءي وءءال اءه يواسي ءلاسرلل ديءءلالا ىوتسم (ديءء لىلءأ=5، ديءء لىلءأ=1)
- ءلاسرللا لىدعت ني كمت
- "لئاسرلل ءفاك ني كمت" ل URL ءباتك ءءاع لىل ني يعتب مت
- [category_لمءءم \$ لىلءال]: لىل اءبسم ءوضوملا رىيغء

Policies									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	BLOCKLIST	Disabled	Disabled	(use default)	Disabled	BLOCKLIST_QUARANTINE	Disabled	(use default)	
2	ALLOWLIST	Disabled	(use default)	(use default)	Disabled	(use default)	Disabled	(use default)	
3	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SDR	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop ...	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ...	Graymail Detection Unsubscribe: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE DKIM_FAILURE SPF_HARDFAIL EXECUTIVE_SPOOF ...	Retention Time: Virus: 1 day Other: 4 hours	Not Available	

ضروع م جهن ل عام س أ

عن م ل ة م ئ اق د ي ر ب جهن

ة ي ام ح ل " ا ن ث ت س ا ب ، ت ا م د خ ل ا ع ي م ج ل ي ط ع ت ع م ر ط ح ل ا ة م ئ اق د ي ر ب جهن ن ي و ك ت م ت ا ر ج ا ة ط س ا و ب ي و ت ح م ل ا ة ي ف ص ت ل م ا ع ل ل ا ت ا ط ا ب ت ر ا و ، " ة ر ا ض ل ل ا ج م ا ر ب ل ل ا ن م ة م د ق ت م ل ل ا ل ع ل .

ب ح و م س م ل ا د ي ر ب ل ا جهن

ي و ت ح م ل ا ة ي ف ص ت ل م ا و ع و ل ط ع م Graymail و AntiSpam ل ع AllowList د ي ر ب جهن ي و ت ح ي و URL_QUARANTINE_MALICIOUS و URL_REWRITE_SUSPICIOUS ل ة ن ك م م ل ل URL_INAPPROPRIATE و DKIM_FAILURE و SPF_HARDFAIL و Executive Spooft و DOMAIN_SPOOF و SDR و TG_RATE_LIMIT و ا ة ي ف ص ت ل م ا و ع ا و ا ه ر ا ت خ ت ي ت ل ا ي و ت ح م ل ا ة ي ف ص ت ل م ا و ع ا و ا ه ر ا ت خ ت ي ت ل ا .

ALLOW_SPOOF د ي ر ب جهن

ن ي ك م ت ع م ، ة ن ك م م ل ا ة ي ض ا ر ت ف ا ل ا ت ا م د خ ل ا ة ف ا ك ل ع ALLOW_SPOOF د ي ر ب جهن ي و ت ح ي و URL_QUARANTINE_MALICIOUS ل ا ي و ت ح م ل ا ة ي ف ص ت ل م ا و ع URL_REWRITE_SUSPICIOUS و URL_INAPPROPRIATE و SDR و ا ة ي ف ص ت ل م ا و ع ا و ا ه ر ا ت خ ت ي ت ل ا .

ر د ا ص ل ا د ي ر ب ل ا جهن

ل ل ل ث ا م م ي ض ا ر ت ف ا ل ا جهن ل ل ن ي و ك ت م ت

ي ة ا و ش ع ل ا د ي ر ب ل ا ة ح ف ا ك م

ل ط ع م

ت ا س و ر ي ف ل ا ة ح ف ا ك م

- " X. س ا ر ن ي م ض ت " ر ا ي ت خ ل ا ل ا ة ن ا خ د ي د ح ت ا ا غ ل ل ط ق ف ت ا س و ر ي ف ل ا ص ح ف : ل ل ا س ر ل ل ا ص ح ف
- " ي ر خ ا ت ا ه ج " ن ي ك م ت ب م ق ، ر خ ا م ا ل ع ا > ة م د ق ت م ت ا ر ا ي خ : ل ل ا س ر ل ل ا ع ي م ج ل ة ب س ن ل ا ب (ي ر ا ي ت خ ل ا) ك ي د ل /SOC ل و و س م ل ل ا ل ا ص ت ا ة ه ج ل ي ن و ر ت ك ل ل ا ل ا د ي ر ب ل ل ا ن ا و ن ع ن ي م ض ت ب م ق و

ة ر ا ض ل ل ا ج م ا ر ب ل ل ا ن م ة م د ق ت م ل ا ة ي ا م ح ل ا

- ط ق ف ف ل م ل ا ة ع م س ن ي ك م ت
- س ا ر ة ف ا ض ا و م د ق ت م س ا ر م د خ ت س ا : ل د ع م ل ا د ح ل ع ي ة و ض ل ل ا ح س م ل ل ا ة ل ب ا ق ر ي غ ت ا ا ر ج ا " ج ي ح ص " : ة م ي ق ل ل ، X-TG-RATElimit : ة ل ا س ر ل ل ا ل ل ا ص ص خ م
- ل ل ا ص ص خ م س ا ر ة ف ا ض ا و Advanced م د خ ت س ا : ة ر ا ض ل ل ا ج م ا ر ب ل ل ا ت ا ق ف ر م ت ا ذ ل ل ا س ر ل ل ا

"عروض جمارب نع فشكلا مت": عميقللا، X-TG-OUTBOUND: ةلاسزللا

لبيميارغ

- لطمع م

يوتحمللا ةيفصت لم اوع

- وأ TG_OUTBOUND_MALICIOUS لبق نم اهراتخت يتللا يوتحمللا ةيفصت لم اوع ديحت مت مت وأ ACCOUNT_TAKEOVER وأ EXTERNAL_SENDER_REMOVE وأ STRIP_SECRET_HEADER وأ CONTENT.

يشفتللا ةيفصت لم اوع

- لطمع م

DLP

- DLP نيوكتو DLP صيخرت يلا اذانتسا، نيكمت

يخأ تاداعل

(سيماوقلا > ديربلا تاسايس) سيماوقلا

- هتعارمو Sexual_Content و ةاذبللا سوماق نيكمت
- ةفاك مادختساب ينورتكللا ديربلا نع فيزمللا فشكلل Executive_FED سوماق عاشنلا ةيفيذيفنتلا عامسألا
- هارت ام بسح اهريغ وأ ةديقملا ةيحاتفملا تاملكلل ةيفاضا سيماوق عاشناب مق نيماألا يف مكحتلا، ةئيبللا، جهنلل ايرورض

(ةهوجللا مكحت رصانع > ديربلا تاسايس) ةهوجللا مكحت رصانع

- لصفمك TLS معد نيوكتب مق، يضارثفالا لاجملا
- لقأ دودح نييعتو بيولا ديربلا لاجملا تاهجو ةفاضلا كنكمي
- [يف مكحتلا تاداعل](#) ليلد [مادختساب رداصللا ديربلل لدعمللا ديحت ليلد](#) ةعجارم اءارلا تامولعمللا نم ديزم يلع لوصحلل [ةهوجللا](#)

Destination Control Table							Items per page 20
Add Destination...							Import Table
Domain ▲	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
.protection.outlook.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	<input type="checkbox"/>
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	<input type="checkbox"/>
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	<input type="checkbox"/>
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	<input type="checkbox"/>
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	Off	Default	
Export Table							Delete
<p>* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</p> <p>^ DANE will not be enforced for domains that have SMTP Routes configured.</p>							

يوتحمل اةيفصت لم اوع

ىل اوع وجرلا ىجرى، يوتحمل اةيفصت لم اوع لوح اةيفاضا تامول عم ىلع لوصحلل: اةطالم نم بس انملا رادص اىل ىلع لوصحلل [مدختس مل ا ل ل د](#) يف "يوتحمل اةيفصت لم اوع" اهرش نب تمق يتل Cisco نم اةنم اىل ينورت كل اىل اةربل اةباوبل AsyncOS.

ا دراوال يوتحمل اةيفصت لم اوع

URL_QUARANTINE_MALICIOUS

طرشل: URL: URL-REPUTATION(-10.00, -6.00, "bypass_url", 1, 1)

اوار اىل: ("URL_MALICIOUS")

URL_REWRITE_SUSPICIOUS

طرشل: URL: URL-REPUTATION(-5.90, -5.60, "bypass_urls", 0, 1)

اوار اىل: URL Reputation: url-reputation-proxy-redirect(-5.90, -5.60, "", 0)

بسانم ريغ url_

رثكأ وأ دحاو طرش تقباطت اذا : قيبطتلا دعاق نييعت *

لزع-خسن ؛ رصانعلا لزع : ءارجإلا (SDR_DATA)

tg_rate_limit

طرشلا ("x-tg-rateLimit") سَأر ؛ رخآ سَأر : طرشللا

لجسلا لاخدا ؛ لجسلا لاخدا ةفاضلا : ءارجإلا ("x-tg-limit: \$files names")

BlockList_Quarantine

طرشلا (ال ب) :

يحصلا رجحلا ؛ يحصلا رجحلا : ءارجإلا ("BLOCKLIST")

Order	Filter Name	Description Rules Policies	Duplicate	Delete
1	URL_QUARANTINE_MALICIOUS	URL_QUARANTINE_MALICIOUS: if (url-reputation{-10.00, -6.00, "bypass_urls", 1, 1}) { quarantine("URL_MALICIOUS"); }		
2	URL_REWRITE_SUSPICIOUS	URL_REWRITE_SUSPICIOUS: if (url-reputation{-5.90, -5.60, "bypass_urls", 0, 1}) { url-reputation-proxy-redirect{-5.90, -5.60, "", 0}; }		
3	URL_INAPPROPRIATE	URL_INAPPROPRIATE: if (url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)) { duplicate-quarantine("INAPPROPRIATE_CONTENT"); }		
4	DKIM_FAILURE	DKIM_FAILURE: if (dkim-authentication == "hardfail") { duplicate-quarantine("DKIM_FAIL"); }		
5	SPF_HARDFAIL	SPF_HARDFAIL: if (spf-status == "fail") { duplicate-quarantine("SPF_HARDFAIL"); }		
6	EXECUTIVE_SPOOF	EXECUTIVE_SPOOF: if (forged-email-detection("Executive_FED", 90, "")) AND (header("X-IronPort-SenderGroup") != "(?)allowspoof") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); duplicate-quarantine("FORGED_EMAIL"); }		
7	DOMAIN_SPOOF	DOMAIN_SPOOF: if (header("X-Spoof")) { duplicate-quarantine("ANTI_SPOOF"); }		
8	SDR	SDR: if (sdr-reputation (['awful', '*']) OR (sdr-age ("days", <, 5, "")) { duplicate-quarantine("SDR_DATA"); }		
9	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-RATELIMIT")) { log-entry("X-TG-RATELIMIT: \$filenames"); }		
10	BLOCKLIST_QUARANTINE	BLOCKLIST_QUARANTINE: if (true) { quarantine("BLOCKLIST"); }		
11	SAMPLE_ATTACHMENT_BLOCK	SAMPLE_ATTACHMENT_BLOCK: if (attachment-filetype == "Executable") OR (attachment-filename == "\\.(386)ad ade adp asp bas bat chm cmd com cpl crt exe hta ins isp jse lnk mdb mdc msc msh msp msq pif reg scr sct shb shs url vbs vbs vss vst vsw ws wsc wsf wsh)\$") { duplicate-quarantine("BLOCK_ATTACHMENTS"); drop(); }		
12	SAMPLE_SPF_SOFTFAIL	SAMPLE_SPF_SOFTFAIL: if (spf-status == "softfail") { duplicate-quarantine("SPF_SOFTFAIL"); }		
13	SAMPLE_MACRO	SAMPLE_MACRO: if (macro-detection-rule (['Adobe Portable Document Format', 'Microsoft Office Files', 'OLE File types'])) { quarantine("MACRO"); }		
14	SAMPLE_ATTACHMENT_PROTECTED	SAMPLE_ATTACHMENT_PROTECTED: if (attachment-protected) { log-entry("Encrypted: \$MID"); }		
15	SAMPLE_LANGUAGE_UNKNOWN	SAMPLE_LANGUAGE_UNKNOWN: if (message-language == "unknown") { edit-header-text("Subject", "(.*)", "[SUSPICIOUS]\\1"); }		
16	SAMPLE_INAPPROPRIATE_CONTENT	SAMPLE_INAPPROPRIATE_CONTENT: if (dictionary-match("Profanity", 1)) OR (dictionary-match("Sexual_Content", 1)) { quarantine("INAPPROPRIATE_CONTENT"); }		
17	SAMPLE_REPLY-TO_MISMATCH	SAMPLE_REPLY-TO_MISMATCH: if (header("reply-to")) AND (header("reply-to") != ""^\$envelopefrom\$") { add-heading("SAMPLE_REPLY-TO_WARN"); log-entry("REPLY-TO MISMATCH"); }		
18	SAMPLE_EXTERNAL_SENDER	SAMPLE_EXTERNAL_SENDER: if (subject != "[EXTERNAL]") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); }		
19	SAMPLE_COUNTRY_FILTER	SAMPLE_COUNTRY_FILTER: if (geolocation-rule (['Canada'])) { log-entry("From Canada"); }		

ةرداصللا يوتحمللا ةيفصت لامواع

Tg_Outbound_Malicious

راض جم انرب == ("X-TG-OUTBOUND") سَأر ؛ رخآ سَأر : طرشللا

لزع (TG_OUTBOUND_MALWARE) : ءارجإلا

ةقباسلا تاسلجلل Cisco نم نمآلا ينورتكلإلا ديربلا تاسرامم لضفأ يطغت ةينقت
([CCO لودل ليجست بلطتي Cisco Live](#)): ةرايز يجري، لوصولو

- BRKSEC-2131 - قيقدل طبضلاو تاسرامملا لضفأ Cisco: نم ينورتكلإلا ديربلا نامأ
- BRKSEC-2131 - ينورتكلإلا كدير قاطن ديدحتب مق
- ديربلا نامأل مدقتملا اهحاصلو اعاطخال فاشكتسأ - ينورتكلإلا ديربلا حالصإ
Cisco - BRKSEC-3265 نم ينورتكلإلا
- Cisco - Devnet-2326 نم ينورتكلإلا ديربلا نامأل API لمكت تايلمع
- Cisco - BRKSEC-1025 نم ةباحسلل ينورتكلإلا ديربلا نامأل مادختساب SAAs ديرب ةبلع تامدخ نيئات
- TECSEC-2345 - قيقدل طبضلاو تاسرامملا لضفأ: ينورتكلإلا ديربلا نامأ
- Cisco - TECSEC-2345 نم ينورتكلإلا ديربلا نامأل عم يعافد فقوم ذاختإ - اديج سيل 250
- Cisco Domain Protection و Cisco Advanced Phishing Protection: ةدافتسإ صقأ قيقحت
BRKSEC-1243 - ينورتكلإلا ديربلا نامأل يف ةيلاتلا ةقبطل نم
- نامأل يف ةيلاتلا ةقبطل نم ةدافتسإ صقأ مدختسنل "فوبس" ل راصتخإ SPF سيل
DGTB-BRKSEC-2327 - ينورتكلإلا ديربلا

ةيفاضا تامولعم

Cisco نم ةنمآلا ينورتكلإلا ديربلا ةرابع قيثوت

- [رادصلا تاطحالم](#)
- [مدختسملال ليلد](#)
- [يعجرملا CLL ليلد](#)
- [Cisco نم ةنمآلا ينورتكلإلا ديربلا ةباوبل تاقيبطتلا ةجرب ةهجاو ةجرب ةلدأ](#)
- [Cisco نم ةنمآلا ينورتكلإلا ديربلا ةرابع يف مدختسملال حوتفملا ردصملا](#)
- [Cisco نم يوتحملال نامأل يرهاظلا زاھجلا تيبثت ليلد](#) (vESA رادصلا نمضتي)

ةنمآلا ينورتكلإلا ديربلا ةباحس ةرابع قيثوتو

- [رادصلا تاطحالم](#)
- [مدختسملال ليلد](#)

Cisco نم بيولا ريومو نمآلا ينورتكلإلا ديربلا قيثوتو

- [قفاوتلا ةفوفصمو رادصلا تاطحالم](#)
- [مدختسملال ليلد](#)
- [Cisco Secure Email و Web Manager ل تاقيبطتلا ةجرب ةهجاو ةجرب ةلدأ](#)
- [Cisco نم يوتحملال نامأل يرهاظلا زاھجلا تيبثت ليلد](#) (vSMA ةينقت نمضتي)

Cisco نم نمآلا حتنملا قيثوتو

- [Cisco نم ةنمآلا عيراشملا ةمئاق ةيمست ةينب](#)

ةلص تاذا تامولعم

- [Cisco نم نمآلا ینورتكلاللا دیربلا نامأ عم قفاوتلا](#)
- [نمآ ینورتكلاللا دیرب: ضرعلا فصو](#)
- [Cisco Universal Cloud تاحلطم](#)
- [Cisco نم تالیزنتلاو م عدلا](#)
- [ةمدقتم تامولعمو SPF تاساسا: OpenSPF \[یجراخ\]](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إامئاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل