Cisco IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®ãƬ¬ã,¤ãƤ2ãƒˆãƳãƒ€ã

High

ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƪãƼID : cisco-sa-20080924-l2tp

CVE-2008-3813

åˆ€å…¬é–‹æ—¥ : 2008-09-24 16:00

ãƒ€ãƼã,¸ãƧãƳ 1.1 : Final

CVSSã,¹ã,³ã,¢ : 7.8

å›žé€ç– : No Workarounds available

Cisco ãƒ€ã,° ID : CSCsh48879

æ—¥æœ¬èªžã€«ã,^ã,‹æƒ…å ±ã¯ã€è‹±èªžã€«ã,^ã,‹åŽŸæ–‡ã®é€žå…¬å¼€ã€

æ¦‚è¦

Cisco IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®Layer 2 Tunneling Protocol(L2TP)ã€®å®Ÿè£…ã€«ã€¯è„†å¼±æ€§ã€Œå˜åœ¨ã€—ã€€é™€å®šã•ã,Œã€ŸCisco IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƪãƪãƼã,¹ã€«å½±éŸ¿ã,’ä¸Žã€ˆã€¾ã€™ã€,

ãƬ¬ã,¤ãƤ2ãƒ€ãƼãƒ€ãƣãƫãƗ—ãƩã,¤ãƙ™ãƼãƈãƒ€ãƒƫãƈãƯãƼã,¯(L2VPN)ã€€ãƬ¬ã,¤ãƤ2ãƒˆãƳã Group Bidding Protocol(SGBP)ã€€ã€Šã,ˆã€³Cisco Virtual Private Dial-Up Networks(VPDN)ã€ªã€©ã€€Cisco IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢å†…ã€§L2TPç®¡ç€†ãƇãƼãƢãƳãƗãƫã,»ã,¹ã,’æœ‰åŠ¹ã€«ã€™ã,‹æ©Ÿèƒ½ã

ã€“ã€®è„†å¼±æ€§ã€¯ã€€ç‰¹å^¥ã€«å·§å¦™ã€«ç´°å·¥ã€•ã,Œã€ŸL2TPãƒã,±ãƫãƈã,’å‡¦ç€†ã€

ã,·ã,¹ã,³ã€¯ã€“ã€®è„†å¼±æ€§ã€«å¯¾å‡¦ã€™ã,‹ã,½ãƒ•ãƈã,¦ã,§ã,¢ã,¢ãƫãƗãƼãƈã,’ãƪãƪãƼ

ã€“ã€®è„†å¼±æ€§ã,’è»½æ›ã€™ã,‹å›žé€ç–ã€Œã€,ã,Šã€¾ã€™ã€,

ã€“ã€®ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƪã€¯ã€€https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-l2tp ã€§å…¬é–‹ã€•ã,Œã€¦ã€„ã€¾ã€™ã€,

æ³¨ï¼š2008å¹´9月24æ—¥ï¼ˆ24æ—¥æœ¬æ™‚é–“ï¼‰ã€®IOSã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƪãƒ€ãƳãƒ‰ãƒ«å…¬é–‹ã€«ã€¯ã€€12ä»¶ã€® IOSã,½ãƒ•ãƈã,¦ã,§ã,¢ã€®è„†å¼±æ€§ã€«å¯¾å‡¦ã€—ã€€1ã€¤ã€®ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƪã€¯Cisco Unified Communications Managerã€®è„†å¼±æ€§ã€«å¯¾å‡¦ã€—ã€¾ã€™ã€,å€„ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƪã€«ã€¯ã€€ã€“ã

å€„ãƒ‰ã,ãƒ¥ãơãƳãƈã€¸ã€®ãƪãƳã,¯ã€¯æ¡ã€®ã€¨ã€Šã,Šã€§ã€™ã€,

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosips
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-cucm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sccp
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosfw

è©²å½“è£½å“

è©²å½“ã™ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã®12.2ã¾ãŸã¯12.4ã®Cisco IOSã‚·ã‚¹ãƒ†ãƒ ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã®ãƒªãƒªãƒ¼ã‚¹ã‚’å®Ÿè¡Œã—ã€ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ãŒè¨å®šã•ã‚Œã¦ã„ã‚‹å ´åˆã«ã®ã¿ã€ã‚·ã‚¹ãƒ†ãƒ ãŒè„†å¼±æ€§ã®å½±éŸ¿ã‚’å—ã‘ã¾ã™ã€‚

è„†å¼±æ€§ã®ã‚ã‚‹è£½å“

ãƒ‡ãƒã‚¤ã‚¹ãŒè„†å¼±æ€§ã®ã‚ã‚‹IOSã‚·ã‚¹ãƒ†ãƒ ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã‚’å®Ÿè¡Œã—ã¦ã„ã‚‹ã‹ã©ã†ã‹ã‚’åˆ¤æ–ã™ã‚‹ã«ã¯ã€ãƒ‡ãƒã‚¤ã‚¹ã§**mgmt daemon**ã‚³ãƒžãƒ³ãƒ‰ã‚’å®Ÿè¡Œã—ã¾ã™ã€‚

ã‚·ã‚¹ãƒ†ãƒ ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’確認するには、**version**ã‚³ãƒžãƒ³ãƒ‰ã‚’入力します。Cisco IOS ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã€ŒInternetwork Operating System Softwareã€‍ã‚‚ã—ãã¯ã€ŒIOSã€‍ã¨è¨¼ç¤ºã•ã‚Œã‚‚ã™ã‚‹ã€å‡ºåŠ›ã®æ¬¡ã®è¡Œã§ã€ã¤ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’å¤šãã®Cisco ãƒ‡ãƒã‚¤ã‚¹ã§ã¯ **show version** ã‚³ãƒžãƒ³ãƒ‰ã‚’実行します。

æ¬¡ã®ä¾‹ã¯ã€Cisco IOSã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹12.4(11)T2ã‚’実行しているデãƒã‚¤ã‚¹ã‚’示しています。

<#root>

```
Router#
```

show version

```
Cisco IOS Software, 7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(11)T2, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 01-May-07 04:19 by prod_rel_team
```

Cisco IOSãƒªãƒªãƒ¼ã‚¹ã®å'½å••è¦•å‰‡ã®è©³ç´°ã«ã¤ã„ã¦ã¯ã€http://www.cisco.com/wa Paper: Cisco IOS Reference Guideã€‚ã¨ã¨ã„ã†ãƒ‰ã‚¥ãƒ¡ãƒ³ãƒˆã‚'å•,ç…§ã—ã¦ã••ã• ã••ã„ã€,

ãƒ—ãƒã‚»ã‚¹**L2TP mgmt daemon**ã•Œãƒ‡ãƒ•ã,¤ã,¹ã•§å®Ÿè¡Œã••ã,Œã•¦ã„ã,‹ã•‹ã•©ã•†ã•‹ã,'ç¢ºèª•ã•™ã,‹ã•«ã **processes**ã,'ç™ºè¡Œã•—ã•¾ã•™ | **include L2TP** ï¼^æ³¨ï¼šã,³ãƒžãƒ³ãƒ‰ã•§ã•¯å¤§æ–‡å—ã•¨å°•å—ã•ŒåŒºå^¥ã••ã,Œã•¾ã•™ï¼‰ã€, å‡ºåŠ›ã•‹ã,‰ãƒ—ãƒã,¹å••**L2TP mgmt daemon**ã•®è¡Œã•Œè¿"ã••ã,Œã•Ÿå ´å•^ã€•ã••ã••ã•®ãƒ‡ãƒ•ã,¤ã,¹ã•«ã•¯è„†å¼±æ€§ã•Œ

```
Router#show processes | include L2TP
 158 Mwe 62590FE4             4           3    133322900/24000  0 L2TP mgmt daemon
Router#
```

L2TPç®¡ç•†ãƒ‡ãƒ¼ãƒ¢ãƒ³ã•¯ã€•L2TPãƒ—ãƒãƒˆã,³ãƒ«ã,'å^©ç"¨ã•™ã,‹ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã,¯ã•«å° **running-config**ã•Œå•«ã•¾ã,Œã•¦ã•„ã,‹å ´å•^ã€•ã••ã•®ãƒ‡ãƒ•ã,¤ã,¹ã•¯L2TP mgmtãƒ‡ãƒ¼ãƒ¢ãƒ³ã,'èµ·å‹•ã•—ã•¦ã•Šã,Šã€•è„†å¼±ã•§ã•™ã€,

- ãƒ‡ãƒ•ã,¤ã,¹ã•«Virtual Private Dial-Up Network(VPDN)ã•Œè¨å®šã••ã,Œã•¦ã•„ã,‹ã€, ã,³ãƒžãƒ³ãƒ‰**vpdn enable**ã•Œãƒ‡ãƒ•ã,¤ã,¹è¨å®šã•«è¡¨ç¤ºã••ã,Œã•¾ã•™ã€,
- ãƒ‡ãƒ•ã,¤ã,¹ã•ŒL2TPã•¾ã•Ÿã•¯L2TPv3ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆé–‹å§‹VPDNãƒˆãƒ³ãƒ•ãƒªãƒ³ã, ã,³ãƒžãƒ³ãƒ‰**pseudowire** ***peer-ip-address vcid*** pw-class ***pw-class-name***ã•Œãƒ‡ãƒ•ã,¤ã,¹è¨å®šã•«è¡¨ç¤ºã••ã,Œã•¾ã•™ã€,
- ãƒ‡ãƒ•ã,¤ã,¹ã•«Stack Group Bidding

Protocol(SGBP)ã€Œè¨å®šã€•ã‚Œã€¦ã€„ã‚‹ã€‚
ã‚³ãƒžãƒ³ãƒ‰**sgbp group** ***group-name***
ã€Œãƒ‡ãƒ•ã‚©ãƒ«ãƒˆè¨å®šã€«è¡¨ç¤ºã€•ã‚Œã¾ã™ã€‚

- L2TPã‚·ã‚°ãƒŠãƒªãƒ³ã‚°ãƒ†ãƒ³ãƒ—ãƒ¬ãƒ¼ãƒˆã€Œå®šç¾©ã€•ã‚Œã€¦ã€„ã‚‹ã€‚
  ã‚³ãƒžãƒ³ãƒ‰**l2tp-class** ***l2tp-class name***
  ã€Œãƒ‡ãƒ•ã‚©ãƒ«ãƒˆè¨å®šã€«è¡¨ç¤ºã€•ã‚Œã¾ã™ã€‚
- ãƒ¬ã‚¤ãƒ¤2ãƒˆãƒ³ãƒãƒ«ãƒãƒˆã‚³ãƒ«ãƒ™ãƒ¼ã‚¹ãƒžãƒƒãƒ—ã¯ã€¨è¨å®šã•ã‚Œã‚ãƒ‡ãƒ•ã‚©ã‚¤
  æ“¬ä¼¼å›žç·šã‚¯ãƒ©ã‚¹ã€Œæ“¬ä¼¼å›žç·šã€¯ãƒ©ã‚¹ã€¹å••ã‚³ãƒžãƒ³ãƒ‰ã¯ã€¨è€æ£å„ªã«é©©ç”¨ã•

è„†å¼±æ€§ã‚’å«ã‚“ã§ã„ãªã„ã“ã¨ã‚’確èª

Ciscoã€Œè£½å“—ã§ã¯ã€„ã‚‹ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒ»ãƒªãƒªãƒ¼ã‚¹ã«ã€¯ã€„ã‚‹ã€‚

- Cisco IOSãƒ•ã‚¡ãƒŸãƒªã‚’実行ã—ã¦ã„ã‚‹ãƒ‡ãƒã‚¤ã‚¹ã‚¹ã€•æ¬¡ã®ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
- Cisco IOS XR ã¯è©²å½“ã—ã¾ã›ã‚“ã€‚
- Cisco IOS XEã¯å½±éŸ¿ã‚’å—ã‘ã¾ã›ã‚“ã€‚

ä»–ã®ã‚·ã‚¹ãƒ†ãƒ ã§è£½å“«ã«Šã„ã¦ã€€ã“ã®ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã®å½±éŸ¿ã‚’å—ã

è©³ç´°

RFC2661ã€€L2TPã€€ã«Šã‚ˆã³RFC3931ã§æ–‡æ›¸åŒ–ã•ã‚Œã¦ã„ã„ã‚‹L2TPv3ã¯ã€€æ—¢å˜

è©²å½“ã™ã‚‹Cisco IOSãƒ•ã‚¡ãƒŸãƒªã®12.2ã€Šã‚ˆã³12.4ã‚’å®Ÿè¡Œã—ã€€ã€€L2TP mgmt daemonãƒ—ãƒã‚»ã‚¹ã‚’実行ã—ã¦ã„ã‚‹ãƒ‡ãƒã‚¤ã‚¹ã¯ã€€ç‰¹å^¥ã«å·§å¦™ã«ç´°

L2TPãƒ—ãƒãƒˆã‚³ãƒ«ã‚’å^©ç”¨ã—ã¦ã€¦ã€Cisco IOSå†…ã§L2TP mgmtãƒ‡ãƒ¼ãƒ¿ãƒ‘ã‚¹ã‚’èµ·å‹•ã™ã‚‹ã€æ©Ÿèƒ½ã€Œã€„ã€ã‚‹ã€Šã¾ã™ã€‚ã€“ã‚Œã‚‰ã

ã€“ã®è„†å¼±æ€§ã¯ã€Cisco Bug ID CSCsh48879(ç™»éŒ²ãƒ¦ãƒ¼ã‚¶ãƒ¼å°‚ç”¨)ã¨ã—ã¦æ–‡æ›¸åŒ–ã•ã‚Œã€Common Vulnerabilities and Exposures(CVE)IDã¨ã—ã¦CVE-2008-3813ã€Œå‰²ã‚Šå½“ã¦ã¦ã„ã‚‹ã‚‰ã‚Œã¦ã„ã¾ã™ã€‚

å›žé¿ç–

ã“ã®è„†å¼±æ€§ã«å¯¾ã—ã¦ã¯ã€ã¯ã€Cisco IOSã€Šã‚ˆã³Cisco IOS XEã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã®ã„ã‚ã‚‰ã‚ã‚‹ãƒªãƒªãƒ¼ã‚¹ã«å¯¾ã—ã¦ã€„ã‚‹ã€‚

æ³¨ï¼š
L**2TPã®å®Ÿè£…**ã®ä¿®æ£ ¼ã®ã‚ã‚‹ã€‚ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã‚‰ã€¤ãƒ³ãƒ•ã‚©ãƒ¡ãƒ¼ã‚·ãƒ§ãƒ³ã€¯ã€RFC 1701ã‚’è¨±å¯ã™ã‚‹å¿…è¦ã€Œã€„ã€ã‚‹ã€Šã¾ã™ã€‚é€šä¿¡å…ƒã‚¢ãƒ‰ãƒ¬ã‚¹ã€Œã€—ãƒãƒ•

æ³¨ï¼šL**2**TPv3 over IPã®ã¿ã‚’å®Ÿè£…ã™ã‚‹å ´å^ã¯ã€ã¯ã™ã¹ã¦ã¦ã®UDP

1701ã,'ã€©ã€"ã€‹ã,‰ã€§ã„,ã,¤ãƳãƕãƩã,¹ãƈãƩã,¯ãƒ€ãƣã,¢ãƉãƬã,¹ã€«å¯¾ã€—ã€¦æ‹'å

- ã,¤ãƳãƕãƩã,¹ãƈãƩã,¯ãƒ€ãƣ ã,¢ã,¯ã,»ã,¹ ã,³ãƳãƈãƫãƼãƫ« ãƪã,¹ãƈ ãƒ€ãƫãƈãƯãƼã,¯ã,'é€šé€Žã€™ã,‹ãƈãƩãƕã,£ãƫãƒ,¯ã,'é€®æ–ã€™ã,‹ã€"ã€¨ã€¯ã€—ã€ ãƫãƒ€ã,¤ã,¹ã,'ã,¿ãƼã,²ãƫãƈã€¨ã€—ã€Ÿè¨±å€¯ã€™ã€¹ã€€ã€§ã€¯ã€ªã€„ãƈãƩãƕã Access Control Lists (iACLs) ã€¯ã€€ãƒ€ãƫãƈãƯãƼã,¯ã,»ã,ãƥãªãƫã,£ã€®ãƙã,¹ãƈãƗãƩã,¯ãƫã,£ã,¹ã€§ã€,ã,Šã€ iACL ã€®ä¾‹ã€¯ã€Infrastructure access-list ã€®ä¸€éƨ¨ã€¨ã€—ã€¦è¨å®šã€•ã,Œã,‹ã€¹ã€€ã€§ã€,ã,Šã€€ã,¤ãƳãƕãƩã,¹ãƈãƩã,¯ã IP ã,¢ãƉãƬã,¹ã€®ç¯„å›²ã€«å€«ã€¾ã,Œã,‹ IP ã,¢ãƉãƬã,¹ã,'æŒ€ã€¤å…¨ã€¦ã€®æ©Ÿå™¨ã,'é˜²å¾¡ã€—ã€¾ã€™:

```
!--- Permit L2TP UDP 1701 packets from all trusted
!--- sources destined to infrastructure addresses.
!--- NOTE: This does not prevent spoofed attacks.
!---           To be a full mitigation, no trusted source
!---           addresses should be listed.
!---           Omit this line if using a L2TPv3 over IP implementation only.

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES MASK
   INFRASTRUCTURE_ADDRESSES MASK eq 1701


!--- Deny L2TP UDP 1701 packets from all
!--- sources destined to infrastructure addresses.


access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 1701


!--- If using a L2TPv3 over IP implementation ensure to allow L2TPv3


access-list 150 permit 115 <source_ip_address and mask>
   <destination_ip_address and mask>


!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!--- with existing security policies and configurations
!--- Permit all other traffic to transit the device.


access-list 150 permit ip any any


!--- Apply access-list to all interfaces (only one example shown)


interface serial 2/0
ip access-group 150 in
```

ãƒ›ãƒ¯ã‚¤ãƒˆãƒšãƒ¼ãƒ‘ãƼã€ŽProtecting Your Core: Infrastructure Protection Access Control Listsã€�ã�§ã�¯ã€�ã,¤ãƳãƕ©ã,¹ãƈãƩã,¯ãƒ�ãƣä¿�è·ã,¢ã,¯ã,»ã,¹ãƪã,¹ãƈã�®ã,¬ã,¤ãƫ%

- ã,³ãƳãƈãƫãƼãƫ ãƒ—ãƬãƼãƳ ãƒ�ãƪã,·ãƳã,°ã,³ãƳãƈãƫãƼãƫ«ãƒ—ãƬãƼãƳãƒ�ãƪã,·ãƳã,°(CoPP)ã,'ä½¿ç"¨ã�—ã�¦ã€�ãƇãƒ�ã,¤ã,¹ã�¸ã€IOS ã,½ãƕãƈã,¦ã,§ã,¢ ãƪãƪãƼã,¹ 12.0Sã€�12.2SXã€�12.2Sã€�12.3Tã€�12.4ã€�ã�Šã,ˆã�³ 12.4T ã�¯ã€�CoPP æ©Ÿèƒ½ã,'ã,µãƒ�ãƼãƈã�—ã�¦ã�„ã�¾ã�™ã€,ç®¡ç�†ã�Šã,ˆã�³ã,³ãƳãƈãƫãƼãƫ«ãƒ—ãƬ CoPP ã,'æ©Ÿå™¨ã�«è¨å®šã�—ã€�æ—¢å˜ã�®ã,»ãƥãƪãƆ£ãƼãƒ�ãƪã,·ãƼã�¨ã,³ãƳãƕ,£ã CoPP ã�®ä¾‹ã�¯ã,¤ãƳãƕ©ã,¹ãƈãƩã,¯ãƒ�ãƣ IP ã,¢ãƒ‰ãƬ,¹ã�®ç¯„å›²å†…ã�«ã�,ã,‹ IP ã,¢ãƒ‰ãƬ,¹ã,'æŒ�ã�¤å…¨ã�¦ã�®æ©Ÿå™¨ã,'ä¿è·ã�™ã,‹ã�Ÿã,ã�«å®šç¾©ã�•ã,Œã CoPP ã�®ä¸€éƒ¨ã�¨ã�—ã�¦å�«ã�¾ã,Œã,‹ã�¹ã��é …ç›®ã�§ã�™:

```
!--- Deny all trusted source L2TP UDP traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will not be policed by the CoPP feature.

!--- NOTE: This does not prevent spoofed attacks.
!---           To be a full mitigation, no trusted source
!---           addresses should be listed.
!---           Omit this line if using an L2TPv3 over IP implementation only.


access-list 111 deny udp TRUSTED_SOURCE_ADDRESSES MASK
   INFRASTRUCTURE_ADDRESSES MASK eq 1701


!--- Permit all L2TP UDP traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature


access-list 111 permit udp any INFRASTRUCTURE_ADDRESSES MASK eq 1701


!--- If using an L2TPv3 over IP implementation ensure not to drop L2TPv3


access-list 111 deny 115 <source_ip_address and mask>
   <destination_ip_address and mask>


!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
```

```
!--- to infrastructure devices

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature


class-map match-all drop-l2tp-class
match access-group 111


!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.


policy-map drop-l2tp-traffic
class drop-l2tp-class
drop


!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane

service-policy input drop-l2tp-traffic
```

ä¸Šè¨˜ã�® CoPP ã�®ä¾‹ã�§ã�¯ã€�"permit" ã,¢ã,¯ã,·ãƒ§ãƒ³ã�§ã�,ã,‹ã,¢ã,¯ã,»ã,¹ã,³ãƒ³ãƒˆãƒãƒ¼ãƒ«ãƒªã,¹ãƒˆã,¨ãƒ³ãƒˆãƒª (ACE) ã�«è©²å½“ã�—ã€�æ”»æ’ƒã�§ã�,ã,‹å�¯èƒ½æ€§ã�®ã�,ã,‹ãƒ‘ã,±ãƒƒãƒˆã�¯ã€�policy-map ã�® "drop" æ©Ÿèƒ½ã�«ã,ˆã,Šå»ƒæ£„ã�•ã,Œã�¾ã�™ã�Œã€�ä¸€æ–¹ã€�"deny" ã,¢ã,¯ã,·ãƒ§ãƒ³(è¨˜è¼‰ã�•ã,Œã�¦ã�„ã�¾ã�›ã,“)ã�«è©²å½“ã�™ã,‹ãƒ‘ã,±ãƒƒãƒˆã�¯ã€�policy-map ã�® "drop" æ©Ÿèƒ½ã�®å½±éŸ¿ã,’å�—ã�‘ã�¾ã�›ã,“ã€‚policy-map ã�®æ§‹æ–‡ã�¯ã€�12.2S ã�¨ 12.0S Cisco IOS ãƒˆãƒ¬ã,¤ãƒ³ã�§ã�¯ç•°ã�ªã,‹ã�®ã�§æ³¨æ„�ã�Œå¿…è¦�ã�§ã�™:

```
policy-map drop-l2tp-traffic
class drop-l2tp-class
police 32000 1500 1500 conform-action drop exceed-action drop
```

CoPPæ©Ÿèƒ½ã�®è¨å®šã�¨ä½¿ç”¨æ–¹æ³•ã�®è©³ç´°ã�«ã�¤ã�„ã�¦ã�¯ã€�æ¬¡ã�®ãƒªã

ãƒ�ãƒƒãƒˆãƒ¯ãƒ¼ã,¯å†…ã�®Ciscoãƒ‡ãƒ�ã,¤ã,¹ã�«é�©ç”¨å�¯èƒ½ã�ªä»–ã�®ç·©å’Œç–«ã�«ã�¤ã

amb-20080924-l2tp)ã,’å�,ç…§ã�—ã�¦ã��ã� ã�•ã„€,

ä¿®æ£æ¸ˆã•¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,'æ¤œè¨Žã•™ã,‹å´å•ˆã•¯ã€•http://www.cisco.com/go/psirt
ã•¨å¾Œç¶šã•®ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã,,å•,ç...§ã•—ã•¦ã€•å••é¡Œã•®è§£æ±ºçŠ¶æ³•ã•¨å®
ã,½ãƒªãƒ¥ãƒ¼ã,·ãƒ§ãƒ³ã,'ç¢ºèªã•—ã•¦ã••ã• ã••ã•„ã€,

ã•„ã•šã,Œã•®å´å•ˆã,,ã€•ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã•™ã,‹æ©Ÿå™¨ã•«å••å^†ã•ªãƒ¡ãƒ¢ãƒªã
Technical Assistance
Centerï¼^TACï¼‰ã•¾ã•Ÿã•¯å¥'ç´„ã,'çµ•ã,"ã•§ã•„ã,‹ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹
ãƒ—ãƒã,¤ãƒ€ãƒ¼ã•«ã•Šå••ã•„å•^ã•›ã••ã• ã••ã•„ã€,

Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®è¡¨ï¼^ä¸‹æŽ²ï¼‰ã•®å•„è¡Œã•«ã•¯ã€•Cisco IOS
ã•®ãƒªãƒªãƒ¼ã,¹
ãƒˆãƒ¬ã,¤ãƒ³ã•Œè¨˜è¼‰ã••ã,Œã•¦ã•„ã•¾ã•™ã€,ç‰¹å®šã•®ãƒªãƒªãƒ¼ã,¹
ãƒˆãƒ¬ã,¤ãƒ³ã•«è„†å¼±æ€§ã•Œã•,ã,‹å´å•ˆã•¯ã€•ä¿®æ£ã,'å•«ã,€æœ€å^•ã•®ãƒªãƒªãƒ¼ã,¹ï¼
1
ä¿®æ£æ¸ˆã•¿ãƒªãƒªãƒ¼ã,¹ã€•å^—ã•«è¨˜è¼‰ã••ã,Œã•¾ã•™ã€,ã€Œæ¨¨å¥¨ãƒªãƒªãƒ¼ã,¹ã€•å
1
ä¿®æ£æ¸ˆã•¿ãƒªãƒªãƒ¼ã,¹ã,^ã,Šå•¤ã•„ï¼‰ãƒˆãƒ¬ã,¤ãƒ³ã•«å•«ã•¾ã,Œã,‹ãƒªãƒªãƒ¼ã,¹ã•Œç¨¼å

ãƒ¡ã,¸ãƒ£ãƒ¼ãƒªãƒªãƒ¼ã,¹	ä¿®æ£æ¸ˆã•¿ãƒª
Affected 12.0-Based Releases	**First Fixed Releaseï¼^ä¿®æ£ã••ã,Œã•Ÿæœ€å^•ã•®ãƒª**
è©²å½"ã•™ã,‹ 12.0 ãƒ™ãƒ¼ã,¹ã•®ãƒªãƒªãƒ¼ã,¹ã•¯ã•,ã,Šã•¾ã•›ã,"ã€,	
Affected 12.1-Based Releases	**First Fixed Releaseï¼^ä¿®æ£ã••ã,Œã•Ÿæœ€å^•ã•®ãƒª**
è©²å½"ã•™ã,‹ 12.1 ãƒ™ãƒ¼ã,¹ã•®ãƒªãƒªãƒ¼ã,¹ã•¯ã•,ã,Šã•¾ã•›ã,"ã€,	
Affected	**First Fixed Releaseï¼^ä¿®æ£ã••ã,Œã•Ÿæœ€å^•ã•®ãƒª**

12.2-Based Releases	
12.2	è„†å¼±æ€§ã•ã•
12.2B	è„†å¼±æ€§ã•ã•
12.2BC	è„†å¼±æ€§ã•ã•
12.2BW	è„†å¼±æ€§ã•ã•
12.2BX	è„†å¼±æ€§ã•ã•
12.2BY	è„†å¼±æ€§ã•ã•
12.2BZ	è„†å¼±æ€§ã•ã•
12.2CX	è„†å¼±æ€§ã•ã•
12.2CY	è„†å¼±æ€§ã•ã•
12.2CZ	è„†å¼±æ€§ã•ã•
12.2DA	è„†å¼±æ€§ã•ã•
12.2DD	è„†å¼±æ€§ã•ã•
12.2DX	è„†å¼±æ€§ã•ã•
12.2EW	è„†å¼±æ€§ã•ã•

12.2EWA	è„†å¼±æ€§ã•ã—
12.2EX	è„†å¼±æ€§ã•ã—
12.2EY	è„†å¼±æ€§ã•ã—
12.2EZ	è„†å¼±æ€§ã•ã—
12.2FX	è„†å¼±æ€§ã•ã—
12.2FY	è„†å¼±æ€§ã•ã—
12.2FZ	è„†å¼±æ€§ã•ã—
12.2IRB	è„†å¼±æ€§ã•ã—
12.2IXA	è„†å¼±æ€§ã•ã—
12.2IXB	è„†å¼±æ€§ã•ã—
12.2IXC	è„†å¼±æ€§ã•ã—
12.2IXD	è„†å¼±æ€§ã•ã—
12.2IXE	è„†å¼±æ€§ã•ã—
12.2IXF	è„†å¼±æ€§ã•ã—
12.2IXG	è„†å¼±æ€§ã•ã—

12.2JA	è„†å¼±æ€§ã•ã—
12.2JK	è„†å¼±æ€§ã•ã—
12.2MB	è„†å¼±æ€§ã•ã—
12.2MC	è„†å¼±æ€§ã•ã—
12.2S	è„†å¼±æ€§ã•ã—
12.2SB	è„†å¼±æ€§ã•ã—
12.2SBC	è„†å¼±æ€§ã•ã—
12.2SCA	è„†å¼±æ€§ã•ã—
12.2SE	æ³¨ï¼š12.2(37)SEã‚ˆã‚Šå‰ã•®ãƒªãƒªãƒ¼ã‚¹ã«ã¯è„†å¼±æ€§ã•ã‚ã‚Šã‚¾ã›ã‚“
12.2SEA	è„†å¼±æ€§ã•ã—
12.2SEB	è„†å¼±æ€§ã•ã—
12.2SEC	è„†å¼±æ€§ã•ã—
12.2SED	è„†å¼±æ€§ã•ã—
12.2SEE	è„†å¼±æ€§ã•ã—
12.2SEF	è„†å¼±æ€§ã•ã—

12.2SEG	è„†å¼±æ€§ã•ã—
12.2SG	æ³¨ï¼š12.2(37)SGã‚ˆã‚Šå‰ã•®ãƒªãƒªãƒ¼ã‚¹ã«ã¯è„†å¼±æ€§ã¯ã‚ã‚Šã¾
12.2SGA	è„†å¼±æ€§ã•ã—
12.2SL	è„†å¼±æ€§ã•ã—
12.2SM	è„†å¼±æ€§ã•ã—
12.2SO	è„†å¼±æ€§ã•ã—
12.2SRA	è„†å¼±æ€§ã•ã—
12.2SRB	12.2(33)SRB1
12.2SRC	è„†å¼±æ€§ã•ã—
12.2SU	è„†å¼±æ€§ã•ã—
12.2SV	è„†å¼±æ€§ã•ã—
12.2SVA	è„†å¼±æ€§ã•ã—
12.2SVC	è„†å¼±æ€§ã•ã—
12.2SVD	è„†å¼±æ€§ã•ã—
12.2SW	è„†å¼±æ€§ã•ã—

12.2SX	è„†å¼±æ€§ã•ã—
12.2SXA	è„†å¼±æ€§ã•ã—
12.2SXB	è„†å¼±æ€§ã•ã—
12.2SXD	è„†å¼±æ€§ã•ã—
12.2SXE	è„†å¼±æ€§ã•ã—
12.2SXF	è„†å¼±æ€§ã•ã—
12.2SXH	è„†å¼±æ€§ã•ã—
12.2SY	è„†å¼±æ€§ã•ã—
12.2SZ	è„†å¼±æ€§ã•ã—
12.2T	è„†å¼±æ€§ã•ã—
12.2TPC	è„†å¼±æ€§ã•ã—
12.2XA	è„†å¼±æ€§ã•ã—
12.2XB	è„†å¼±æ€§ã•ã—
12.2XC	è„†å¼±æ€§ã•ã—
12.2XD	è„†å¼±æ€§ã•ã—

12.2XE	è„†å¼±æ€§ã•ã•
12.2XF	è„†å¼±æ€§ã•ã•
12.2XG	è„†å¼±æ€§ã•ã•
12.2XH	è„†å¼±æ€§ã•ã•
12.2XI	è„†å¼±æ€§ã•ã•
12.2XJ	è„†å¼±æ€§ã•ã•
12.2XK	è„†å¼±æ€§ã•ã•
12.2XL	è„†å¼±æ€§ã•ã•
12.2XM	è„†å¼±æ€§ã•ã•
12.2XN	è„†å¼±æ€§ã•ã•
12.2XNA	è„†å¼±æ€§ã•ã•
12.2XNB	è„†å¼±æ€§ã•ã•
12.2XO	è„†å¼±æ€§ã•ã•
12.2XQ	è„†å¼±æ€§ã•ã•
12.2XR	è„†å¼±æ€§ã•ã•

12.2XS	è„†å¼±æ€§ã•ã•
12.2XT	è„†å¼±æ€§ã•ã•
12.2XU	è„†å¼±æ€§ã•ã•
12.2XV	è„†å¼±æ€§ã•ã•
12.2XW	è„†å¼±æ€§ã•ã•
12.2YA	è„†å¼±æ€§ã•ã•
12.2YB	è„†å¼±æ€§ã•ã•
12.2YC	è„†å¼±æ€§ã•ã•
12.2YD	è„†å¼±æ€§ã•ã•
12.2YE	è„†å¼±æ€§ã•ã•
12.2YF	è„†å¼±æ€§ã•ã•
12.2YG	è„†å¼±æ€§ã•ã•
12.2YH	è„†å¼±æ€§ã•ã•
12.2YJ	è„†å¼±æ€§ã•ã•
12.2YK	è„†å¼±æ€§ã•ã•

12.2YL	è„†å¼±æ€§ã�ªã�—
12.2YM	è„†å¼±æ€§ã�ªã�—
12.2YN	è„†å¼±æ€§ã�ªã�—
12.2YO	è„†å¼±æ€§ã�ªã�—
12.2YP	è„†å¼±æ€§ã�ªã�—
12.2YQ	è„†å¼±æ€§ã�ªã�—
12.2YR	è„†å¼±æ€§ã�ªã�—
12.2YS	è„†å¼±æ€§ã�ªã�—
12.2YT	è„†å¼±æ€§ã�ªã�—
12.2YU	è„†å¼±æ€§ã�ªã�—
12.2YV	è„†å¼±æ€§ã�ªã�—
12.2YW	è„†å¼±æ€§ã�ªã�—
12.2YX	è„†å¼±æ€§ã�ªã�—
12.2YY	è„†å¼±æ€§ã�ªã�—
12.2YZ	è„†å¼±æ€§ã�ªã�—

12.2ZA	è„†å¼±æ€§ã�ªã�—
12.2ZB	è„†å¼±æ€§ã�ªã�—
12.2ZC	è„†å¼±æ€§ã�ªã�—
12.2ZD	è„†å¼±æ€§ã�ªã�—
12.2ZE	è„†å¼±æ€§ã�ªã�—
12.2ZF	è„†å¼±æ€§ã�ªã�—
12.2ZG	è„†å¼±æ€§ã�ªã�—
12.2ZH	è„†å¼±æ€§ã�ªã�—
12.2ZJ	è„†å¼±æ€§ã�ªã�—
12.2ZL	è„†å¼±æ€§ã�ªã�—
12.2ZP	è„†å¼±æ€§ã�ªã�—
12.2ZU	è„†å¼±æ€§ã�ªã�—
12.2ZX	è„†å¼±æ€§ã�ªã�—
12.2ZY	è„†å¼±æ€§ã�ªã�—
12.2ZYA	è„†å¼±æ€§ã�ªã�—

Affected 12.3-Based Releases	First Fixed Releaseï¼ˆä¿®æ£ã•ã‚Œã•Ÿæœ€å^ã®ã®ãƒª
è©²å½“ã™ã‚‹ 12.3 ãƒ™ãƒ¼ã‚¹ã®ãƒªãƒªãƒ¼ã‚¹ã¯ã‚ã‚Šã¾ã›ã‚“ã€‚	

Affected 12.4-Based Releases	First Fixed Releaseï¼ˆä¿®æ£ã•ã‚Œã•Ÿæœ€å^ã®ã®ãƒª
12.4	è„†å¼±æ€§ã•ã—
12.4JA	è„†å¼±æ€§ã•ã—
12.4JK	è„†å¼±æ€§ã•ã—
12.4JL	è„†å¼±æ€§ã•ã—
12.4JMA	è„†å¼±æ€§ã•ã—
12.4JMB	è„†å¼±æ€§ã•ã—
12.4JMC	è„†å¼±æ€§ã•ã—
12.4JX	è„†å¼±æ€§ã•ã—
12.4MD	è„†å¼±æ€§ã•ã—
12.4MR	æ³¨ï¼š12.4(11)MRã‚ˆã‚Šå‰ã®ãƒªãƒªãƒ¼ã‚¹ã«ã¯è„†å¼±æ€§ã¯ã‚ã‚Šã¾ã›
12.4SW	12.4(11)SW3

12.4T	æ³¨ï¼š12.4(11)Tã,^ã,Šå‰¯ã•®ãƒªãƒªãƒ¼ã,¹ã•«ã•¯è„†å¼±æ€§ã•¯ã•,ã,Šã•¾ã•›ã,“ã
12.4XA	è„†å¼±æ€§ã•ªã•—
12.4XB	è„†å¼±æ€§ã•ªã•—
12.4XC	è„†å¼±æ€§ã•ªã•—
12.4XD	è„†å¼±æ€§ã•ªã•—
12.4XE	è„†å¼±æ€§ã•ªã•—
12.4XF	è„†å¼±æ€§ã•ªã•—
12.4XG	è„†å¼±æ€§ã•ªã•—
12.4XJ	è„†å¼±æ€§ã•,ã,Š(æœ€å^•ã•®ä¿®æ£ã•¯12.4T)
12.4XK	è„†å¼±æ€§ã•ªã•—
12.4XL	è„†å¼±æ€§ã•ªã•—
12.4XM	è„†å¼±æ€§ã•ªã•—
12.4XN	è„†å¼±æ€§ã•ªã•—
12.4XP	è„†å¼±æ€§ã•ªã•—
12.4XQ	è„†å¼±æ€§ã•ªã•—

12.4XT	è„†å¼±æ€§ã�ªã�—
12.4XV	è„†å¼±æ€§ã�,ã,Šã€,TACã�«ã�Šå•�ã�„å�ˆã,�ã�›ã��ã� ã�•ã�„
12.4XW	12.4(11)XW1
12.4XY	è„†å¼±æ€§ã�ªã�—
12.4XZ	è„†å¼±æ€§ã�ªã�—
12.4YA	è„†å¼±æ€§ã�ªã�—

ä¸�æ£åˆ©ç”¨äº‹ä¾‹ã�¨å…¬å¼�ç™ºè¡¨

Cisco PSIRT
ã�§ã�¯ã€�æœ¬ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�«è¨˜è¼‰ã�•ã,Œã�¦ã�„ã,‹è„†å¼±æ€§ã�®ä¸�æ£åˆ©ç”

ã�“ã�®è„†å¼±æ€§ã�¯ã€�ã,·ã,¹ã,³ã�®ç¤¾å†…ã,¹ãƒˆã,¹ãƒˆã�«ã,ˆã�£ã�¦ç™ºè¦‹ã�•ã,Œã�¾ã�—ã

URL

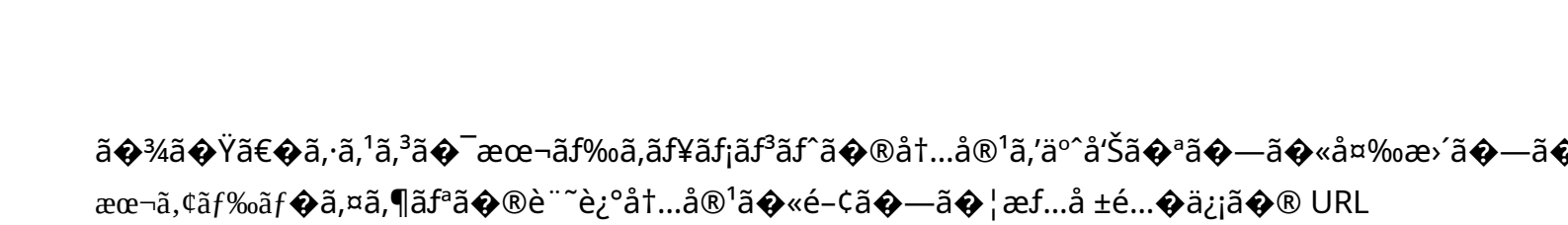
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-l2tp

æ”¹è¨,å±¥æ´

ãƒªãƒ“ã,¸ãƒ§ãƒ³ 1.1	2009å¹´4月16æ—¥	ç¡®å®ˆã•ã,Œã�Ÿã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒ†ãƒ¼ãƒ–ãƒ«ã,¸ã,®å®,ç
ãƒªãƒ“ã,¸ãƒ§ãƒ³ 1.0	2008å¹´9月24æ—¥	å^ç‰ˆãƒªãƒªãƒ¼ã,¹

å^©ç”¨è¦ç´„

本ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�¯ç„¡ä¿è¨¼ã�®ã,,ã�®ã�¨ã�—ã�¦ã"æ��ä¾›ã�—ã�¦ã�Šã,Šã€
本ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�®æ…å ±ã�Šã,ˆã�³ãƒªãƒ³ã,¯ã�®ä½¿ç"¨ã�«é–¢ã�™ã,‹è²¬ä»»ã�®ä¸€

ã 
æœ¬ã‚ªãƒ•ã,¤ãƒªãƒ³ã®è¨˜è¿°å†…容ã®¹ã«é–¢ã—ã¦ã¦ æ…é…ä¿¡ã® URL
ã,'çœ•ç•¥ã—ã€å˜ç‹¬ã®»è¼‰ã„æ„è¨³ã,'æ–½ã—ã—Ÿå ´å^ã€å½“ç¤¾ã®Œç®¡ç•
ã“ã®ãƒ‰ã,ãƒ¥ãƒ³ãƒˆã®æ…å ±ã¯ã€·ã,¹ã,³è£½å“•ã®ã,¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã,¶ã,'å¯¾è±¡ã

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。