ãƒªãƒãƒ¼ãƒ‰æ™‚ã«ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚Œ

Informational

ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªID : cisco-sa-asaftd-aclconfig-wVK52f3z
å^åŧ¬é–‹æ—¥ : 2023-07-27 16:00
æœ€çµ‚æ›´æ–°æ—¥ : 2023-07-27 16:38
ãƒãƒ¼ã‚¸ãƒ§ãƒ³ 1.1 : Final
å›žé¿ç– : No workarounds available
Cisco ãƒã‚° ID : CSCwe64043 CSCwf71606

æ—¥æœ¬èªžã«ã‚ˆã‚‹å ±å‘Šèªžã«ã‚ˆã‚ŽåŽŸæ–‡ã®é€žå…¬å¼ã

æ¦‚è¦

Ciscoé©©å¿œåž‹ã‚»ã‚ãƥãƪãƣã‚£ã‚¢ã‚¯ã‚»ã‚¹ãƳ(ASA)ã‚½ãƒ•ãƈã‚¦ã‚§ã‚Šã‚ˆã³Firepowe

ã“ã®å•é¡Œã¯€ACLã®ãƒ–ãƼãƈæ™‚ã«ãƗãƪã‚°ãƩãƠã•ã‚Œã‚‹éš›ã«ç™ºç”Ÿã™ã‚‹ã‚ˆã†ã«ãªã‚Šã¾ã—ãŸã€‚ã“ã®å¯¾å‡¦ã™ã‚‹ã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ã‚¢ãƪãƼã‚¹ã‚’

ã“ã®ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƪã¯€æ¡ˆã®ãƪãƳã¯ã€ˆçº²è²ã§ã••ã¾ã™ã€‚
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-aclconfig-wVK52f3z

è„†å¼±æ€§ã®ã‚ã‚‹è£½å“

ã“ã®å•é¡Œã¯€Cisco ASAã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ãƪãƼã‚¹9.18.1ä»¥é™ã‚ã¾ã—ã¯€Cisco FTDã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ãƪãƼã‚¹7.2.0ä»¥é™ã‚’å®Ÿè¡Œã—ã¦ã„ã‚‹ã‚·ã‚¹ãƳè£½å“ã«å½±

Cisco Bug ID CSCwe64043ã¯€æ¡ˆã®ãƪãƳã¯ã«ã‚Šã‚‘ã“ã®å•é¡Œã®å‹•ä½œã«å½±éŸ

- Cisco ASAã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ãƪãƼã‚¹9.18.3.39ã€ž9.18.3.46ã€ž9.19.1.12
- Cisco FTDã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ãƪãƼã‚¹7.2.4

Cisco ASAãƪãƪãƼã‚¹	Cisco FTDãƪãƪãƼã‚¹	è¨å®šã‚®ä¾‹å˜é–¢ä¿
9.18.1 ä»¥é™ 9.19.1 ä»¥é™	7.2.0 ä»¥é™	ã‚ªãƗã‚¸ã‚§ã‚¯ãƈã‚°ãƫãƼãƗ
9.18.3.39	7.2.4	ã‚ªãƗã‚¸ã‚§ã‚¯ãƈã‚°ãƫãƼãƗã

Cisco ASAãƒªãƒªãƒ¼ã‚¹	Cisco FTDãƒªãƒªãƒ¼ã‚¹	è¨å®šã®ä¾‹å˜é–¢ä¿‚
9.18.3.46 9.19.1.12		«ã‚ˆã‚‹OGSã‚¢ã‚¯ã‚»ã‚¹ã‚¹ãƒ†å¾¡

å½±éŸ¿ã‚’å—ã‘ã‚‹ã‚™ã‚™ã„è¨å®šä¾‹ã«ã¤ã„ã¦ã¯ã€è©³ç´°ã€ã‚»ã‚¯ã‚·ãƒ§ãƒ³ã‚’å‚ç…§ã—ã¦ãã ã•ã„ã€‚

CSCwe64043ã®å½±éŸ¿ã‚’å—ã‘ã‚‹ãƒªãƒªãƒ¼ã‚¹ã§ã®å•ä½œ

Cisco ASAã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹9.18.1ä»¥é™ã®ã‚ˆã†Cisco FTDã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹7.2.0ä»¥é™ã§ã§ã¯ã€ã“ã®å•é¡Œã¯ãƒ‡ãƒã‚¤ã‚¹

ã“ã®å•é¡Œã®åŽŸå› ã§ã‚¨ãƒ¼ã‚¿ãƒƒãƒ—ã‚¬ãƒ³ãƒ•ã‚£ã‚®ãƒ¥ãƒ¬ãƒ¼ã‚·ãƒ§ãƒ³ã§

ã‚ªãƒ–ã‚¸ã‚§ã‚¯ãƒˆã‚°ãƒ«ãƒ¼ãƒ—ã®å¤±æ•—ã™ã‚‹ã¨ã¨ãƒ‡ãƒã‚¤ã‚¹ã®

```
Specified group object (name) does not exist
*** Output from config line xxxx, " group-object name..."
```

ã“ã®ã¨ãƒ©ãƒ¼ãƒ¡ãƒƒã‚»ãƒ¼ã‚¸ã¯ã€ãƒ‡ãƒã‚¤ã‚¹ã®

CSCwe64043ã®å½±éŸ¿ã‚’å—ã‘ã‚‹ãƒªãƒªãƒ¼ã‚¹ã§ã®å•ä½œ

OGS ACLæœ€é©©åŒ–æ©Ÿèƒ½ã€Œæœ‰åŠ¹ã«ã—ã¦ã„ã‚‹Cisco ASAã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹9.18.3.39ã€œ9.18.3.46ã€œ9.19.1.12ã€Šã‚ˆã³Cisco FTDã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹7.2.4ã€§ã€¯ã€€ã€“ã®å•é¡Œã¯ãƒ‡ãƒã‚¤ã‚¹ã‚¬ãƒ¼ãƒ‰ã‚¨ãƒ³ã‚¸ãƒ³ã€ã¾ãŸã¯ãƒžãƒ«ãƒã‚³ãƒ³ãƒ†ã‚¯ã‚¹ãƒˆãƒ¢ãƒ¼ãƒ‰ã§

ã“ã®å•é¡Œã¯ã€OGS ACLæœ€é©©åŒ–æ©Ÿèƒ½ãŒæœ‰åŠ¹ã«ãªã£ã¦ã„ã‚‹ã€ASAã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹9.18.1ä»¥é™ã®ã€Šã‚ˆã³Cisco FTDã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹7.2.0ä»¥é™ã®æ–°ã—ã„ã‚¤ãƒ³ã‚¹ãƒˆãƒ¼ãƒ«ã€©ã€ASAã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹9.18(x)ãƒªãƒªãƒ¼ã‚¹ãƒˆãƒŽãƒ¼ãƒˆï¼šASA 9.18(1)ã€®æ–°æ©Ÿèƒ½ã€‚ã‚’å‚ç…§ã—ã¦ãã ã•ã„ã€‚

OGS ACLæœ€é©©åŒ–è¨å®šã®æ±ºå®š

OGS ACLæœ€é©©åŒ–è¨å®šã‚’ç¢ºèªã™ã‚‹ã«ã¯ã€ãƒ‡ãƒã‚¤ã‚¹ã®CLIã§**show**

running-config object-group-searchã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç"¨ã—ã¾ã™ã€,æ¬¡ã®ä¾‹ã«ã¯ACLæœ€é©©åŒ–æ©Ÿèƒ½ãŒæœ‰åŠ¹ã«ã•ã£ã¦ã„ã,‹ã•ã,Œã,«å±±é™ºã«ã•ã,
running-config object-group-searchã,³ãƒžãƒ³ãƒ‰ã®å‡ºåŠ›ã,'ç¤ºã—ã¦ã¦ã¾ã™ã€,

```
<#root>

#
show running-config object-group-search


object-group-search access-control
```

ã•“ã•®ã,³ãƒžãƒ³ãƒ‰ã•§ç©ºã•®å‡ºåŠ›ã•Œè¿"ã••ã,Œã,‹ã•‹ã€•no object-group-search access-controlã•®å‡ºåŠ›ã•Œè¿"ã••ã,Œã,‹å ´å•^ã•¯ã€•OGS ACLæœ€é©©åŒ–æ©Ÿèƒ½ãŒç„¡åŠ¹ã«ã•ªã•£ã•¦ã•Šã,Šã€•ãƒ‡ãƒ•ã,¤ã,¹ã•¯ã•“ã•®å••

è„†å¼±æ€§ã•Œå˜åœ¨ã•™ã,‹ã,·ã,¹ã,³ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã•«ã•¤ã•„ã•¦ã•¯ã€•ã•“

è„†å¼±æ€§ã,'å•«ã,“ã•§ã•„ã•ªã•„ã•“ã•¨ã•Œç¢ºèª•ã••ã,Œã•Ÿè£½å“•

ã•“ã•®ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƒªã•®è„†å¼±æ€§ã•®ã•,ã,‹è£½å“•ã,»ã,¯ã,·ãƒ§ãƒ³ã•«è¨˜è¼‰ã••ã,Œ

ã,·ã,¹ã,³ã•§ã•¯ã€•ã•“ã•®å••é¡Œã•ŒCisco Firepower Management Center(FMC)ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•«ã•¯å½±éŸ¿ã,'ä¸Žã•^ã•ªã•„ã•“ã•¨ã,'ç¢ºèª•ã•—ã•¦ã•„

è©³ç´°

ACLã•¯ã€•ãƒ‡ãƒ•ã,¤ã,¹ã•¨ã•®é–“ã€•ã•Šã,^ã•³ãƒ‡ãƒ•ã,¤ã,¹ã,'çµŒç"±ã•™ã,‹ãƒ•ãƒƒãƒˆãƒ¯ãƒ

æ³¨ï¼šãƒªãƒ–ãƒ¼ãƒˆæ™‚ã•«ãƒ‡ãƒ•ã,¤ã,¹ã•§ã•“ã•®å••é¡Œã•Œç™ºç"Ÿã•™ã,‹ã•‹ã•©ã•†ã•‹ã,'
group #1ã•¯object-group #2ã,'ãƒ¡ãƒ•ãƒ•ã•¨ã•—ã•¦ä½¿ç"¨ã•—ã•¾ã•™ã•Œã€•ã,¹ãƒ¼ãƒˆã,¢ãƒƒãƒ—ã,³ãƒ³ãƒ•ã,£ã,®ãƒ group #2ã•¯å¾Œã•§ã•®ã•¿ä½œæˆ•ã••ã,Œã•¾ã•™ã€,ã•“ã,Œã•«ã,^ã,Šã€•ãƒªãƒ–ãƒ¼ãƒˆæ™‚ã•«

CSCwe64043ã•®å½±éŸ¿ã,'å•—ã•'ã•ªã•„ãƒªãƒªãƒ¼ã,¹ã•§ã•®å½±éŸ¿ã,'å•—ã

ã•“ã•®å••é¡Œã•¯ã€•Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹9.18.1ä»¥é™•ã•¾ã•Ÿã•¯Cisco FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹7.2.0ä»¥é™•ã,'å®Ÿè¡Œã•—ã•¦ã•„ã,‹ã,·ã,¹ã,³è£½å“•ã•«å½±éŸ

group network group1-
dmzã€Œå€,ç...§å¾Œã€«ã,¹ã,¿ãƒ¼ãƒˆã,¢ãƒƒãƒ—ã,³ãƒ³ãƒ•ã,£ã,®ãƒ¥ãƒ¬ãƒ¼ã,·ãƒ§ãƒ³ã€«å€«ã¾ã,Œã
group network group1-
dmzã€¯ãƒãƒ¼ãƒ‰ã€•ã,Œã€šã€€è¦ªã‚ãƒ–ã,¸ã,§ã,¯ãƒˆã,°ãƒ«ãƒ¼ãƒ—ãƒ€ãƒƒãƒˆãƒ¯ãƒ¼ã,¯ã€ŒAã€€

<#root>

```
!
Object-group network group2-dmz
Object-group network group3-dmz
!
object-group network â€œAâ€€
```

group-object group1-dmz

```
 group-object group2-dmz
 group-object group3-dmz
!
```

Object-group network group1-dmz

ã€“ã,Œã€«ã,ˆã,Šã€€æœ€åˆ€ã€®ãƒªãƒãƒ¼ãƒ‰æ™,ã€«ã€®ã€¿ã€€æ¬¡ã€®ã,³ãƒ³ãƒ•ã,½ãƒ¼ãƒ«ã,¨

<#root>

```
Specified group object (
```

group1-dmz

```
) does not exist
*** Output from config line xxxx, " group-object
```

group1-dmz

```
..."
```

CSCwe64043ã€®å½±éŸ¿ã,'å€—ã€'ã,‹ãƒªãƒªãƒ¼ã,¹ã€§ã€®è„†å¼±æ€§ã€Œå˜åœ

Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹9.18.3.39ã€€9.18.3.46ã€€9.19.1.12ã€Šã,ˆã€³Cisco FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹7.2.4ã€¯CSCwe64043ã€®å½±éŸ¿ã,'å€—ã€'ã€€**object-group-search access-control**
ACLæœ€é€©åŒ–æ©Ÿèƒ½ã€Œæœ‰åŠ¹ã€«ã€ªã€£ã€¦ã€„ã,‹å ´å€ˆã€®ã€¿ã€€ã€“ã€®ã,¢ãƒ
group-search access-controlã€Œè¨å®šã€•ã,Œã€¦ã€Šã,Šã€€Object-group network group1-dmzã€Œå€,ç...§å¾Œã€«ã,¹ã,¿ãƒ¼ãƒˆã,¢ãƒƒãƒ—ã,³ãƒ³ãƒ•ã,£ã,®ãƒ¥ãƒ¬ãƒ¼ã,·ãƒ§ãƒ³ã€«ã€,ã,Šã€¾ã€ access-

listã®å‡ºåŠ›ã«è¡¨ç¤ºã•ã,Œã¾ã›ã,“ã€,

```
<#root>

!

object-group-search access-control


.
.
.
!
!
Object-group network group2-dmz
Object-group network group3-dmz
!

object-group network â€œAâ€

 group-object group1-dmz
 group-object group2-dmz
 group-object group3-dmz
!

Object-group network group1-dmz


!
```

ã“ã®ã,·ãƒŠãƒªã,ªã¯ã€ãƒªãƒãƒ¼ãƒ‰å‰Šé™¤ã€ã™ã¹ã¦ã¦ã®ACLã«Œæ£ã—ã••é©©

access-list

CLIã,³ãƒžãƒ³ãƒ‰ã®å‡ºåŠ›ã,’æ¯”è¼ƒã™ã,‹ã“ã¨ã§ç¢ºèªã§ã§ã¾ã™ã€,æ¬¡ã®ä¾‹ã

```
<#root>

# show access-list
access-list Inside_in line 1 extended deny ip object-group A any (hitcnt=0) 0xd90bfe1b


access-list Inside_in line 1 extended deny ip v4-object-group A(2147483650) any4(2147549186) (hitcnt=0)


  access-list Inside_in line 1 extended deny ip v4-object-group A(2147483650) any6(2147549187) (hitcnt=0


access-list Inside_in line 2 extended permit ip object-group B any (hitcnt=0) 0x8beb7d31
  access-list Inside_in line 2 extended permit ip v4-object-group B(2147483652) any4(2147549186) (hitcnt
  access-list Inside_in line 2 extended permit ip v4-object-group B(2147483652) any6(2147549187) (hitcnt
```

æ¬¡ã®ä¾‹ã¯ã€ãƒªãƒãƒ¼ãƒ‰å¾Œã®å‡ºåŠ›ã,’ç¤ºã—ã¦ã„ã¾ã™ã€,ACLã«Œæ£ã——

<#root>

#

show access-list

```
access-list Inside_in line 1 extended deny ip object-group A any (hitcnt=0) 0xd90bfe1b
access-list Inside_in line 2 extended permit ip object-group B any (hitcnt=0) 0x8beb7d31
  access-list Inside_in line 2 extended permit ip v4-object-group B(2147483652) any4(2147549186) (hitcnt
  access-list Inside_in line 2 extended permit ip v4-object-group B(2147483652) any6(2147549187) (hitcnt
```

å›žé¿ç–

ã"ã®å•é¡Œã«å¯¾å‡¦ã™ã‚‹å›žé¿ç–¯ã¯ã‚ã‚Šã¾ã›ã‚“ã€‚

ã"ã®ã»ã¯ã‚·ã§§ãƒ³ã®æƒ…å ±ã¯ã€€å®Ÿè¡Œã‚³ãƒ³ãƒ•ã‚£ã‚®ãƥãƬãƼã‚·ãƧãƳã«å«ã¾ã¾

1. ä¿®æ£æ¸ˆã¿ãƒªãƒªãƼã‚¹ã«ã‚¢ãƥãƗãƒ¼ãƉã—ã¦ã¦ã„ã,ã€æ¬ è½ã—ã¦ã¦ã„ã
2. ãƒªã‚«ãƒã‚¹ãƒ—ã‚·ãƧãƳã®1ã¤ã‚’å®Ÿè£…ã—ã¦ã„ã¾ã€æ—¢ã®ã‚¯ãƒ©ã‚¹ã‚¿ãƒ¼ã«
3. ACLã«Æ‰‹å‹•ã§å›žé¿ã•ã,Œã€Ÿå¾Œã€ã€ã"ã®ã‚¢ãƉ‰ãƒ•ã‚¤ã‚¸ãƪãƳã®ã€Œ
   FMCã¾ãŸã¯Cisco Cloud-Delivered
   FMC(cdFMC)ã«ã‚ˆã£ã¦ç®¡ç†ã•ã,Œã‚‹Cisco
   FTDãƒ‡ãƒã‚¤ã‚¹ã§ã€è¨å®šã®å›žé¿ã•ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®ã,¢ãƒƒãƗãƼã,°ãƪ

Cisco FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƪãƪãƼã,¹7.2.0 ï½ž 7.3.1ã®å›žé¿ã,ªãƗã,·ãƒ§ãƳ([CSCwe64043](#)ã®å½±éŸ¿ã,'å—ã'ã'ªã„)

ã"ã,Œã,‰ã®ãƪãƪãƼã,¹ã§ã¯ã€ã,¹ã,¿ãƼãƈã,¢ãƒƒãƗãƼã,³ãƳãƒ•ã,£ã,®ãƥãƬãƼã,·ãƒ§ãƳã

- Cisco FMCã¾ãŸã¯Cisco cdFMCã«ã,ˆã£ã¦ç®¡ç†ã•ã,Œã¦ã„ã,‹ãƒ‡ãƒã‚¤ã,¹ã®å ´å^ã€å½±éŸ¿ã,'å—ã
  FTDãƒ‡ãƒã‚¤ã,¹ã,'ãƪãƒãƼã‰ã™ã,‹ã¯Ÿã³ã«ã€ã,¯ã,»ã,¹ã,³ãƳãƈãƒãƼãƫãƒãƪã,
  Deployã,'å®Ÿè¡Œã—ã¾ã™ã€,
- Cisco FMCã€Cisco cdFMCã€ã¾ãŸã¯Cisco Defense Orchestratorã«ã,ˆã£ã¦ç®¡ç†ã•ã,Œã,‹ãƒ‡ãƒã‚¤ã,¹ã«ã¤ã„ã¦ã¯ã€Cisco FMCã¾ãŸã¯Cisco cdFMC UIã‹ã‚‰ã,¯ã,»ã,¹ã,³ãƳãƈãƒãƼãƫãƒãƪã,·ãƼ(ACP)ã®**Force Deploy**ã,'å®Ÿè¡Œã—ã¾ã™ã€,

Cisco Defense Orchestratorã,'æ‹¡ã—ã¦Cisco FDM(Firepower Device Manager)ã¾ãŸã¯Cisco FDMã«ã,ˆã£ã¦ç®¡ç†ã•ã,Œã,‹Cisco FTDãƒ‡ãƒã‚¤ã,¹ã¯ã€ã"ã®å•é¡Œã®å½±éŸ¿ã,'å—ã'ã¾ã›ã‚“ã€,

Cisco

FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹7.2.4ã€®ãƒªã,«ãƒ€ãƒªã,ªãƒ—ã,·ãƒ§ãƒ³(CSCwe6404

ã€“ã€®ãƒªãƒªãƒ¼ã,¹ã€§ã€¯ã€€ACLã€¯ã,¹ã,¿ãƒ¼ãƒˆã,¢ãƒƒãƒ—ã,³ãƒ³ãƒ•ã,£ã,®ãƒ¥ãƒ¬ãƒ¼ã,·ãƒ§ãƒ³ã€

- Cisco FMCã€¾ã€Ÿã€¯Cisco cdFMCã€«ã,ˆã€£ã€¦ç®¡ç€†ã€•ã,Œã€¦ã€„ã,‹ãƒ‡ãƒ€ã,¤ã,¹ã€®å´å€ˆã€¯ã€€å½±éŸ¿ã,’å FTDãƒ‡ãƒ€ã,¤ã,¹ã€«é–¢é€£ä»˜ã€’ã€¦å±•é–‹ã€™ã,‹æ–¹æ³•ã€Œæ¨¥å¥¨ã€•ã,Œã€¾ã€™ã€‚
- Cisco FMCã€¾ã€Ÿã€¯Cisco cdFMCã€«ã,ˆã€£ã€¦ç®¡ç€†ã€•ã,Œã,‹ãƒ‡ãƒ€ã,¤ã,¹ã€«å¯¾ã€™ã,‹å^¥ã€®å›žå¾©ã,ªãƒ—ã, FTDãƒ‡ãƒ€ã,¤ã,¹ã€«å±•é–‹ã€™ã,‹ã€“ã€¨ã€§ã€™ã€‚å•€é¡Œã€®ã€,ã,‹ãƒ«ãƒ¼ãƒ«ã,’å^¤å^¥ã FTDãƒ‡ãƒ€ã,¤ã,¹ã€§**show access-list** CLIã,³ãƒžãƒ³ãƒ‰ã,’ä½¿ç”¨ã€—ã€¦ã€€æ³¨é‡ˆã€®ã€¿ã,’è¡¨ç¤ºã€™ã,‹3è¡Œä»¥ä¸Šã€®è¡Œã€

```
<#root>

#

show running-config access-list

.
.
.

access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: TEST - Mandatory


access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: TEST1


access-list CSM_FW_ACL_ remark rule-id 268437506: ACCESS POLICY: TEST - Mandatory


access-list CSM_FW_ACL_ remark rule-id 268437506: L7 RULE: TEST2


access-list CSM_FW_ACL_ remark rule-id 268437504: ACCESS POLICY: TEST - Default
access-list CSM_FW_ACL_ remark rule-id 268437504: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268437504 event-log flow-endsrc_rule_26
```

- Cisco FMCã€Cisco cdFMCã€ã€¾ã€Ÿã€¯Cisco Defense Orchestratorã€«ã,ˆã€£ã€¦ç®¡ç€†ã€•ã,Œã,‹ãƒ‡ãƒ€ã,¤ã,¹ã€«å¯¾ã€—ã€¦ã€¯ã€€Cisco FMCã€«ã,ˆã€£ã€¦ã€®ã€¿ç®¡ç€†ã€•ã,Œã,‹Cisco FTDãƒ‡ãƒ€ã,¤ã,¹ã€«é–¢ã€—ã€¦èª¬æ˜Žã€•ã,Œã€¦ã€„ã,‹å›žå¾©æ‰‹é †ã€¨å€Œã€˜æ‰

Cisco Defense Orchestratorã,’æ€è¼‰ã€—ã€ŸCisco FDM(Firepower Device Manager)ã€¾ã€Ÿã€¯Cisco FDMã€«ã,ˆã€£ã€¦ç®¡ç€†ã€•ã,Œã,‹Cisco FTDãƒ‡ãƒ€ã,¤ã,¹ã€¯ã€€ã€“ã€®å•€é¡Œã€®å½±éŸ¿ã,’å€—ã€’ã€¾ã€›ã,“ã€,

Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹9.18.1ã€‹ã,‰9.18.3.39ã€¾ã€§ã€®ãƒªã,«ãƒ€ãƒª

ã€“ã,Œã,‰ã€®ãƒªãƒªãƒ¼ã,¹ã€§ã€¯ã€€ã€,¹ã,¿ãƒ¼ãƒˆã,¢ãƒƒãƒ—ã,³ãƒ³ãƒ•ã,£ã,®ãƒ¥ãƒ¬ãƒ¼ã,·ãƒ§ãƒ³ã€

CLIã€¾ã€Ÿã€¯Cisco Adaptive Security Device Manager(ASDM)ã,'ä½¿ç"¨ã€—ã€¦ç®¡ç€†ã€•ã,Œã€¦ã€„ã,‹Cisco ASAã€®å ´å€ˆã€¯ã€€ã€€ã,Œã€žã,Œã€®è¦ªã,ªãƒ–ã,¸ã,§ã,¯ãƒˆã,°ãƒ«ãƒ¼ãƒ—ã€®ä¸‹ã€«ã€€ä¸

- ãƒ‡ãƒ•ã,¤ã,¹ã€®CLIã€‹ã,‰running-configã,'ã,³ãƒ"ãƒ¼ã€—ã€€ãƒãƒ¼ã,«ãƒ«ãƒžã,·ãƒ³ä¸Šã€®**config1.txt**ï¼ˆã€¾ã€Ÿã€¯ä»»æ„ã€®
- ãƒ€ãƒƒã,¯ã,¢ãƒƒãƒ—è¨å®šã€¾ã€Ÿã€¯ä¥å‰‰ã€«ä¿å˜ã€—ã€Ÿè¨å®šã‹ã,‰ã€€æ¯"è
- CLIã€‹ã,‰2ç•ªç›®ã€®è¨å®šã,'ã,³ãƒ"ãƒ¼ã€—ã€€ãƒãƒ¼ã,«ãƒ«ãƒžã,·ãƒ³ä¸Šã€®**config2.txt**ï¼ˆã€
- ãƒ†ã,ã,¹ãƒˆã,¨ãƒ‡ã,£ã,¿ã€¾ã€Ÿã€¯ç«¯æœ«ãƒ™ãƒ¼ã,¹ã€®ç›¸é•ãƒ„ãƒ¼ãƒ«(**diff**ã,„**vimdiff**ã€ªã€
- ç›¸é•ãƒ„ãƒ¼ãƒ«ã€§å¼·è¡¨ç¤ºã•ã,Œã€Ÿç›¸é•ã,'å^†æž€ã€—ã€¾ã€™ã€,é€šå„€ã€è¿½

ASAã€Cisco Security Managerã€«ã,^ã€£ã€¦ç®¡ç€†ã€•ã,Œã€¦ã€„ã,‹å ´å€ˆã€€ç®¡ç€†è€…ã€¯ä»»æ„ã€®å°Žå…¥ Security Managerã€¯ã,¢ã,¦ãƒˆã,ªãƒ–ãƒ³å¤‰æ›´(OOB)ã€Œæœ‰åŠ¹ï¼ˆãƒ‡ãƒ•ã,©ãƒ«ãƒˆï¼‰ã€®å ´å€

Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹9.18.3.39ã€€9.18.3.46ã€€ã€¾ã€Ÿã€¯9.19.1.12ã€

ã€“ã,Œã,‰ã€®ãƒªãƒªãƒ¼ã,¹ã€§ã€¯ã€€ACLã€¯ã,¹ã,¿ãƒ¼ãƒˆã,¢ãƒƒãƒ—ã,³ãƒ³ãƒ•ã,£ã,®ãƒ¥ãƒ¬ãƒ¼ã,·

CLIã€¾ã€Ÿã€¯Cisco ASDMã,'ä½¿ç"¨ã€—ã€¦ç®¡ç€†ã€•ã,Œã,‹ãƒ‡ãƒ•ã,¤ã,¹

CLIã€¾ã€Ÿã€¯Cisco ASDMã,'ä½¿ç"¨ã€—ã€¦ç®¡ç€†ã€•ã,Œã€¦ã€„ã,‹Cisco ASAã€®å ´å€ˆã€€ä¸€èˆ¬çš„ã€«ã€¯ã€€ç®¡ç€†è€…ã€¯å•€é¡Œã€®ã€,ã,‹ã,ªãƒ–ã,¸ã,§ã,¯ãƒˆã,°ãƒ« **access-list**
CLIã,³ãƒžãƒ³ãƒ‰ã,'ç¹°ã,Šè¿"ã€—ã€¦ã,¢ã,¯ã,»ã,¹ãƒªã,¹ãƒˆãƒ«ãƒ¼ãƒ«ã,'å›žå¾©ã€™ã,‹å¿…è¦ã€Œã€ **3ã€Œã,ªãƒ–ã,¸ã,§ã,¯ãƒˆã,°ãƒ«ãƒ¼ãƒ—ãƒ€ãƒƒã‚¯ãƒ¼ãƒ¼ã,¯RISK-NETS**ã€§ä½¿ç"¨ã€•ã,Œã€Ÿå¾Œã€€å®Ÿè¡Œã,³ãƒ³ãƒ•ã,£ã,®ãƒ¥ãƒ¬ãƒ¼ã,·ãƒ§ãƒ³ã€§é †ç•ªã€«ä½¿ç"

```
<#root>

#

show access-list

.
.
```

.

access-list Inside_in line 1 extended deny ip object-group RISK-NETS any (hitcnt=0) 0xd90bfe1b

```
access-list Inside_in line 2 extended permit ip object-group ALLOW-NETS any (hitcnt=0) 0x8beb7d31
  access-list Inside_in line 2 extended permit ip v4-object-group ALLOW-NETS(2147483652) any4(214754918
  access-list Inside_in line 2 extended permit ip v4-object-group ALLOW-NETS(2147483652) any6(214754918
```

#

show running-config | include object|subnet|access

```
object-group network Subnets-1
 network-object object Subnet1A
 network-object object Subnet1B
!
```

object-group network RISK-NETS

```
 group-object Subnets-1
```

group-object Subnets-3

```
!
```

object-group network Subnets-3

```
 network-object object Subnet3A
 network-object object Subnet3B
!
```

å‰Šé¨˜ã®ä¾‹ã§ã¯ã€**RISK-NETS**ã«é–¢é€£ä»˜ã‘ã‚‰ã‚Œã¦ã¦ã„ã‚‹ã™ã¹ã¦ã®ã‚¨ãƒ³ãƒˆãƒªã‚’å‰Šé™¤ã—ã¦ã„ã¾ã™ã€‚**3**ã€Œãƒ¡ãƒƳãƒ¼ã‚¯ã€ã‚‚ã‚Ÿã€ã‚ã‚Ÿã‚ ã—ã€é †ç•ªã€Œæ£ã—ã„ã„ã‚ˆã†ã«è¦‹ãˆã¾ã™ãŒã€**3**ã¯å®Ÿè¡Œã•ã‚Œã¾ã›ã‚“ã€‚ã‚¨ãƳãƼã‚·ãƧãƳã®**RISK-NETS**ã®å¾Œã«æœŸå¾…ã•ã‚Œã¦ã„ã‚‹ã™ã¹ã¦ã®ã‚¨ãƳãƼã‚’å•é¡Œãªãå‰Šé™¤ã—ã¾ã™ã€‚

```
# config t
(config)# object-group network RISK-NETS
(config-network-object-group)# no group-object Subnets-3
(config)# access-list Inside_in line 1 extended deny ip object-group RISK-NETS any
```

Cisco Security Managerã‚’ä½¿ç”¨ã—ã¦å®Ÿçœã•ã‚Œã‚‹ãƒ¡ãƒªãƒƳãƒˆ

Cisco Security Managerã«ã‚ˆã£ã¦å®Ÿçœã•ã‚Œã‚‹Cisco ASAã®ãƪãƳãƪãƪãƳã‚·ãƧãƳæ¬¡ã®ã¨ãŠã‚Šã§ã™ã€‚

- å½±éŸ¿ã‚’å

ï¿—ã€'ã‚‹ãƒ‡ãƒã‚¤ã‚¹ã«é–¢é€£ä»˜ã€'ã‚‰ã‚Œã¦ã¦ã„ã‚‹ç®¡ç†ACPã‚'è¤‡è£½ã€—

- ç®¡ç€†è€…ã€¯ã€€ã€"ã€®å•€é¡Œã€®å½±éŸ¿ã‚'å€—ã€'ã€Ÿå€Œã€˜ACPã€«æ–°ã€—ã

ACLãƒªã‚«ãƒ€ãƒªã€«é–¢ã€™ã‚‹ã‚µãƒ¼ãƒ¼ãƒˆã€Œå¿…è¦ã€ªã€Šå®¢æ§˜ã€¯ã€€Cisco Technical Assistance Center(TAC)ã€¾ã€Ÿã€¯å¥'ç´„ã€—ã€Ÿãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã‚¹ãƒ—ãƒã‚¤ã€«é€£çµ¡ã€™ã‚‹ã€

ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹

ãƒ½ãƒªãƒ¼ã‚¹ã€®ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã‚'æ¤œè¨Žã€™ã‚‹éš›ã«ã€¯ã€¯ã€·ã€¹ã€³ ã€»ã€ãƒ¥ãƒªãƒ†ã‚£ ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒª ãƒŠãƒ¼ãƒ“ã‚²ãƒ¼ã‚¿ãƒ¼ã€®å…¥æ‰‹ã€§ã€ã€ã€·ã€¹ã€³è£½å“"ã€®ã€¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã‚'å®šæœŸçš„ã€«å€,ç ãƒ½ãƒªãƒ¥ãƒ¼ã,·ãƒ§ãƒ³ä¸€å¼¢ã,'ç¢ºèª"ã€—ã€¦ã€ã€ã€•ã€„ã€‚

ã€„ã€šã,Œã€®å´å€^ã,,ã€€ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã€™ã,‹ãƒ‡ãƒã,¤ã,¹ã€«å€€å^†ã€ªãƒ¡ãƒ¢ã Technical Assistance Centerï¼^TACï¼‰ã,,ã€—ã€€ã€¯å¥'ç´„ã€—ã€¦ã€„ã,‹ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹ãƒ—ãƒã,¤ãƒ¼ã

ä¿®æ£æ¸ˆã€ãƒªãƒªãƒ¼ã‚¹

ç™ºè¡Œæ™‚ç‚¹ã€§ã€¯ã€æ¬¡ã€«è¨˜è¼‰ã€•ã,Œã€¦ã€„ã,‹ãƒªãƒªãƒ¼ã,¹æƒ…å ±ã€¯æ£ç¢º ID ã€®è©³ç´°ã,»ã,¯ã,·ãƒ§ãƒ³ã,'å€,ç…§ã€—ã€¦ã€€ã€•ã€„ã€‚

å·¦ã€®å^—ã€¯ã,·ã,¹ã,³ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã,'ç¤ºã€—ã€€å€³ã€®å^—ã€¯ãƒªãƒªãƒ¼ã,¹ã€

Cisco ASAãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼^ä¿®æ£ã€•ã,Œã€Ÿæœ€å^ €ã€®ãƒªãƒªãƒ¼ã,¹ï¼‰
9.18 ã,^ã,Šå‰€	Not affected
9.18	9.18.3.53
9.19	9.19.1.18

Cisco FTD ãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼^ä¿®æ£ã€•ã,Œã€Ÿæœ€å^ €ã€®ãƒªãƒªãƒ¼ã,¹ï¼‰
7.2 ã,^ã,Šå‰€	Not affected
7.2	7.2.4.1 7.2.5 Cisco_FTD_Hotfix_AW-7.2.4.1-1.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_AW-7.2.4.1-1.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_AW-7.2.4.1-1.sh.RE L.tar Cisco_FTD_SSP_FP3K_Hotfix_AW-7.2.4.1-1.sh.RE L.tar

Cisco FTD ãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã•Ÿæœ€åˆ•ã®ãƒªãƒªãƒ¼ã,¹ï¼‰
	Cisco_FTD_SSP_Hotfix_AW-7.2.4.1-1.sh.RE L.tar
7.3	7.3.1.1 (future release)

Product Security Incident Response Teamï¼ˆPSIRT; ãƒ—ãƒãƒ€ã,¯ãƒˆ ã,»ã,ãƒ¥ãƒªãƒ†ã,£
ã,¤ãƒ³ã,·ãƒ‡ãƒ³ãƒˆ ãƒ¬ã,¹ãƒ•ãƒ³ã,¹
ãƒ•ãƒ¼ãƒ ï¼‰ã•¯ã€•ã•“ã•®ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƒªã•«è¨˜è¼‰ã••ã,Œã•¦ã•„ã,‹è©²å½“ã•™ã

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”

å‡ºå…¸

ã•“ã•®å••é¡Œã•¯ã€•Cisco
TACã,µãƒãƒ¼ãƒˆã,±ãƒ¼ã,¹ã•®è§£æ±ºä¸•ã•«ç™ºè¦‹ã••ã,Œã•¾ã•—ã•Ÿã€,

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-aclconfig-wVK52f3z

æ”¹è¨‚å±¥æ´

ãƒãƒ¼ã,¸ãƒ§ãƒ³	èª¬æ˜Ž	ã,»ã,¯ã,·ãƒ§ãƒ³	ã,¹ãƒ†
1.1	ã,ªãƒ–ã,¸ã,§ã,¯ãƒˆã,°ãƒ«ãƒ¼ãƒ—ã•®å½¹å‰²ã,'æ˜Žç¢ºåŒ–ã€,	è¦•ç´„	Final
1.0	å^•å›žå…¬é–‹ãƒªãƒªãƒ¼ã,¹	â€”	Final

å^©ç”¨è¦•ç´„

æœ¬ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƒªã•¯ç„¡ä¿è¨¼ã•®ã,,ã•®ã•¨ã•—ã•¦ã•”æ••ä¾›ã•—ã•¦ã•Šã,Šã€
æœ¬ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƒªã•®æƒ…å ±ã•Šã,^ã•³ãƒªãƒ³ã,¯ã•®ä½¿ç"¨ã•«é–¢ã•™ã,‹è²¬ä»»ã•®ä¸€
ã•¾ã•Ÿã€•ã,¹ã,³ã•¯æœ¬ãƒ‰ã,ãƒ¥ãƒ¡ãƒ³ãƒˆã•®å†…å®¹ã,'äº^å'Šã•ªã•—ã•«å¤‰æ›´ã•—ã
æœ¬ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƒªã•®è¨˜è¿°å†…å®¹ã•«é–¢ã•¦æƒ…å ±é…•ä¿¡ã•® URL
ã,'çœ•ç•¥ã•—ã€•å•˜ç‹¬ã•®è»¢è¼‰ã,„æ„•è¨³ã,'æ–½ã•—ã•Ÿå ´å•^ã€•å½"ç¤¾ã•Œç®¡ç•
ã•“ã•®ãƒ‰ã,ãƒ¥ãƒ¡ãƒ³ãƒˆã•®æƒ…å ±ã•¯ã€•ã,·ã,¹ã,³è£½å“•ã•®ã,¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã,¶ã,'å¯¾è±¡

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。