Cisco Unified Communications Manager 및 Cisco Intercompany Media Engine의 DOS(Denial of Service) 취약성 식별 및 완화

Cisco Unified Communications Manager 및 Cisco Intercompany Media Engine의 DOS(Denial of Service) 취약성 식별 및 완화

자문 ID: cisco-amb-20110824-cucm-ime

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110824-cucm-ime

개정 1.1

최종 업데이트 날짜: 2011년 11월 2일 23:20 UTC (GMT)

2011년 8월 24일 00:00 UTC(GMT) 공개 릴리스의 경우

목차

Cisco의 대응

Applied Mitigation Bulletin PSIRT Security Advisories *Cisco Unified Communications Manager Denial of Service Vulnerabilities* and *Denial of Service Vulnerabilities in Cisco Intercompany* Media Engine Cisco .

취약성 특성

Cisco Unified Communications Manager Intercompany Media Engine . . **Cisco Unified Communications Manager DoS :** . . Unified Communications Manager DoS( ) . Unified Communications Manager 3-way TCP TCP . CVE CVE-2011-2560 .**MTP Cisco Unified Communications Manager DoS :** . . DoS . .

- TCP 5060 SIP(Session Initiation Protocol)
- TCP 5061 SIP over TLS(Transport Layer Security)
- UDP 5060 SIP
- UDP 5061 SIP

. CVE CVE-2011-2561 . **SIP INVITE Cisco Unified Communications Manager DoS :** . . DoS .

- TCP 5060 SIP
- TCP 5061 SIP-TLS over TLS(Transport Layer Security)
- UDP 5060 SIP
- UDP 5061 SIP-TLS

. CVE CVE-2011-2562 .**Cisco Unified Communications Manager Cisco Intercompany Media Engine(IME) with SAF(Service Advertisement Framework) DoS :** . . DoS . .

- TCP 5050 SAF (Cisco Unified Communications Manager)
- TCP 5620 SAF (IME)

CVE CVE-2011-2563 CVE-2011-2564 . , , PSIRT Security Advisories . PSIRT Security Advisories .
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-cucm
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-ime.

완화 기법 개요

Cisco . . .Cisco IOS Software .

- (tACL)
- RPF(Unicast Reverse Path Forwarding)
- IP (IPSG)

IP . RPF IP . RPF .IPSG . , RPF IPSG .Cisco ASA 5500 Series Adaptive Security Appliance Cisco Catalyst 6500 FWSM(Firewall Services Module) .

- (tACL)
- RPF(Unicast Reverse Path Forwarding)
- TCP

IP .Cisco ACE Application Control Engine TCP . .Cisco IPS(Intrusion Prevention System) .Cisco IOS NetFlow .Cisco IOS Software, Cisco ASA, FWSM , Cisco ACE Application Control Engine **show** syslog .Cisco Security MARS(Monitoring, Analysis, and Response System) , .

위험 관리

조직은 표준 위험 평가 및 완화 프로세스를 준수하여 [이 취약성|이러한 취약성]의 잠재적 영향을 확인하는 것이 좋습니다. 분류(Triage)란 성공 가능성이 가장 높은 프로젝트를 분류하고 노력을 우선순위를 정하는 것을 말한다. Cisco는 조직이 정보 보안 팀을 위해 위험 기반 분류 기능을 개발하는 데 도움이 될 문서를 제공했습니다. 보안 취약성 알림에 대한 위험 분류 및 위험 분류 및 프로토타이핑은 조직이 반복 가능한 보안 평가 및 대응 프로세스를 개발하는 데 도움이 될 수 있습니다.

디바이스별 완화 및 식별

: , , , . , . .

- Cisco IOS
- Cisco IOS NetFlow
- Cisco ASA FWSM
- Cisco ACE
- Cisco
- Cisco ,

Cisco IOS : , VPN tACL(transit access control list) . tACL . tACL .tACL TCP UDP 5060 5061 SIP, SAF SIP-TLS . 192.168.60.0/24 2001:DB8:1:60::/64 IPv4 IPv6 , 192.168.100.1(IPv6 2001:DB8:1:100::1) . .tACL :.

```
! !-- Include explicit permit statements for trusted sources !-- that require
access on the vulnerable protocols and ports ! access-list 150 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 access-list 150 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 access-list 150 permit udp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 access-list 150 permit udp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 access-list 150 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5050 access-list 150 permit tcp
```

```
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5620 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list 150 deny deny tcp any 192.168.60.0
0.0.0.255 eq 5060 access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq
5061 access-list 150 deny deny udp any 192.168.60.0 0.0.0.255 eq 5060 access-
list 150 deny deny udp any 192.168.60.0 0.0.0.255 eq 5061 access-list 150
deny deny tcp any 192.168.60.0 0.0.0.255 eq 5050 access-list 150 deny deny
tcp any 192.168.60.0 0.0.0.255 eq 5620 ! !-- Permit or deny all other Layer 3
and Layer 4 traffic in accordance !-- with existing security policies and
configurations ! !-- Explicit deny for all other IP traffic ! access-list 150
deny ip any any ! !-- Create the corresponding IPv6 tACL ! ipv6 access-list
IPv6-Infrastructure-ACL-Policy ! !-- Include explicit permit statements for
trusted sources !-- that require access on the vulnerable protocols and ports
! permit tcp host 2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5060 permit tcp
host 2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5061 permit udp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5060 permit udp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5061 permit tcp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5050 permit tcp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5620 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks to global and !-- link local addresses ! deny tcp
any 2001:DB8:1:60::/64 eq 5060 deny tcp any 2001:DB8:1:60::/64 eq 5061 deny
udp any 2001:DB8:1:60::/64 eq 5060 deny udp any 2001:DB8:1:60::/64 eq 5061
deny tcp any 2001:DB8:1:60::/64 eq 5050 deny tcp any 2001:DB8:1:60::/64 eq
5620 ! !-- Permit other required traffic to the infrastructure address !--
range and allow IPv6 Neighbor Discovery packets, which !-- include Neighbor
Solicitation packets and Neighbor !-- Advertisement packets ! permit icmp any
any nd-ns permit icmp any any nd-na ! !-- Explicit deny for all other IP
traffic to the global !-- infrastructure address range ! deny ipv6 any
2001:DB8:1:60::/64 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic
!-- in accordance with existing security policies and configurations ! ! !--
Apply tACLs to interfaces in the ingress direction ! interface
GigabitEthernet0/0 ip access-group 150 in ipv6 traffic-filter IPv6-
Infrastructure-ACL-Policy in
```

ICMP . CPU . Cisco IOS Software ICMP 500 . ICMP no ip unreachable . ICMP **ip icmp rate-limit unreachableinterval-in**-ms .: IP . RPF(Unicast Reverse Path Forwarding) . RPF IP . IP RPF RPF . RPF ( ) . 3 RPF . Unicast Reverse Path Forwarding Loose Mode . RPF Understanding Unicast Reverse Path Forwarding Applied Intelligence .**IP Source Guard**IPSG(IP source guard) DHCP IP 2 IP . IPSG IP / MAC . IPSG RPF .IPSG DHCP IP .: tACL **show ip access-lists** TCP UDP 5060 5061 SIP SIP-TLS . . **show ip access-lists 150** .

```
router#show ip access-lists 150
Extended IP access list 150
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
    40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5050
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5620
    70 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (5 matches)
    80 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (2 matches)
    90 deny deny udp any 192.168.60.0 0.0.0.255 eq 5060 (7 matches)
    100 deny deny udp any 192.168.60.0 0.0.0.255 eq 5061 (4 matches)
    110 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5050 (6 matches)
    120 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5620 (1 matches)
    130 permit icmp any any nd-ns
    140 permit icmp any any nd-ns
    150 deny ip any any
```

```
router#
```

150 .

- ACE 70 **TCP 5060 SIP 5**
- ACE 80 **TCP 5061 2 SIP-**TLS
- ACE 90 UDP **5060 SIP 7**
- ACE 100 **UDP 5061 SIP 4**
- ACE 110 **TCP 5050 6 SAF**
- ACE 120 **TCP 5620 1** SAF

IPv6 tACL , . ACE syslog Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence . ACE Embedded Event Manager . Embedded Event Manager Applied Intelligence **ID: log** and **log-input** ACL(access control list) ACE . **log-input** IP **.:** CPU . ACL CPU , , ACE .Cisco IOS Software **ip access-list logging interval** *in-ms* ACL . logging **rate-limit** *rate-per-second* [**except** *loglevel*] .ACL CPU Supervisor Engine 720 Supervisor Engine 32 Cisco Catalyst 6500 Series Cisco 7600 Series ACL .ACL ACL __ **.:** RPF show cef interface *type slot/portinternal,* **show ip interface**, **show cef drop**, **show ip cef switching statistics** **show ip traffic** RPF **.:** Cisco IOS Software 12.4(20)T **show ip cef switching** **show ip cef switching statistics** **.: show command | begin** *regex* and **show** *command* **| include** *regex!command modifiers* . Cisco IOS Configuration Fundamentals show .

```
router#show cef interface GigabitEthernet 0/0 internal | include drop

  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#
```

: show cef interface *type slot/port* **internal** CLI . .

```
router#show ip interface GigabitEthernet 0/0 | begin verify

  IP verify source reachable-via RX, allow default, allow self-ping
  18 verification drops
  0 suppressed verification drops
router#
```

```
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route      No_adj  ChkSum_Err
RP            27           0           0          18           0           0
router#
```

```
router#show ip cef switching statistics feature
IPv4 CEF input features:
Path   Feature               Drop    Consume       Punt  Punt2Host Gave route
RP PAS uRPF                    18          0          0          0          0
Total                          18          0          0          0          0
    --      CLI Output Truncated       --
router#
```

```
router#show ip traffic | include RPF
        18 no route, 18 unicast RPF, 0 forced drop
router#
```

show cef drop, **show ip cef switching statistics feature** and **show ip traffic** examples Unicast RPF **18** IP . Cisco Express Forwarding Forwarding Information Base IP Unicast RPF .**Cisco IOS NetFlow: NetFlow** Cisco IOS Cisco IOS NetFlow . .

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000
```

```
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP           236      0.0        12    66      0.0       1.8       4.8
TCP-FTPD           21      0.0     13726  1294      0.0      18.4       4.1
TCP-WWW         22282      0.0        21  1020      0.1       4.1       7.3
TCP-X             719      0.0         1    40      0.0       0.0       1.3
TCP-BGP             1      0.0         1    40      0.0       0.0      15.0
TCP-Frag        70399      0.0         1   688      0.0       0.0      22.7
TCP-other     47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS           582      0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  06 0984 13C4     3
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 13C5     2
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3A 13BA     6
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 13C4     2
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B31 15F4     1
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   11 0B89 13C5     7
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     4
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
router#
```

TCP 5060(16 13C4), 5061(16 13C5), 5050(16 13BA) 5620(16 15F4) UDP 5060(16 13C4) **5061(16 13C5)** SIP, SAF SIP-TLS ! 192.168.60.0/24 . , . UDP 5060 5061 SIP SIP-TLS , .TCP 5060(16 13C4), 5061(16 13C5), 5050(16 13BA) 5620(16 15F4) SIP, SAF SIP-TLS **show ip cache flow | include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_** UDP NetFlow .**TCP**

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  06 0984 13C4     3
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 13C5     2
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3A 13BA     6
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 13C4     2
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B31 15F4     1
router#
```

UDP 5060(16 13C4) 5061(16 13C5) SIP SIP-TLS **show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_** UDP NetFlow .**UDP**

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.17    Gi0/1         192.168.60.97   11 0B89 13C5     7
Gi0/0         192.168.12.185   Gi0/1         192.168.60.239  11 0BD7 13C4     4
router#
```

: IPv6 NetFlow Cisco IOS Cisco IOS IPv6 NetFlow . . Cisco IOS Software 12.4 Cisco IOS . Cisco IOS .

```
router#show ipv6 flow cache
IP packet size distribution (50078919 total packets):
   1-32  64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .990 .001 .008 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 475168 bytes
  8 active, 4088 inactive, 6160 added
  1092984 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  IP Sub Flow Cache, 33928 bytes
  16 active, 1008 inactive, 12320 added, 6160 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x06 0x2001 0x13C4 1464K
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x180A 0x13C5 3456
2001:DB...6A:5BA6 Gi0/0    2001:DB...28::21 Gi0/1    0x3A 0x0000 0x8000 2191
2001:DB...6A:5BA6 Gi0/0    2001:DB...134::3 Gi0/1    0x3A 0x0000 0x8000 1909
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x18C4 0x13C4 4567K
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x3A 0x0000 0x8000 1192
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::2 Gi0/1    0x06 0x160A 0x13C5 1597
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::3 Gi0/1    0x06 0x1610 0x13BA 1001
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x06 0x1634 0x15F4 1292
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::3 Gi0/1    0x3A 0x0000 0x8000 1292
2001:DB...6A:5BA6 Gi0/0    2001:DB...146::3 Gi0/1    0x3A 0x0000 0x8000 1392
2001:DB...6A:5BA6 Gi0/0    2001:DB...144::4 Gi0/1    0x3A 0x0000 0x8000 1493
```

128 IPv6 **terminal width 132 exec** mode . TCP 5060(16 13C4), 5061(16 13C5), 5050(16 13BA) 5620(16 15F4) UDP 5060(16 13C4) **5061(16 13C5)** SIP, SAF SIP-TLS **!** 2001:DB8:1:60::/64 . , . UDP 5060 5061 SIP SIP-TLS , . TCP 5060(16 13C4), 5061(16 13C5), 5050(16 13BA) 5620(16 15F4) SIP, SAF SIP-TLS **show ipv6 flow cache | NetFlow SrcAddress|_06_.*(13C4|13C5|13BA|15F4)_** .**TCP**

```
router#show ipv6 flow cache | include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_
SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x06 0x2001 0x13C4 1464K
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::2 Gi0/1    0x06 0x160A 0x13C5 1597
2001:DB...6A:5BA6 Gi0/0 2001:DB...128::3 Gi0/1 0x06 0x1610 0x13BA 1001
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x06 0x1634 0x15F4 1292
router#
```

IPv6 UDP 5060**(16 0x13C4)** 5061**(16 0x13C5)** SIP SIP-TLS **show ipv6 flow cache | SrcAddress|_11_.*(13C4|13C5)_** NetFlow .**UDP**

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_
SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x180A 0x13C5 3456
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x18C4 0x13C4 4567K
routter#
```

Cisco ASA FWSM : , VPN tACL . tACL . tACL .tACL TCP UDP 5060 5061 SIP, SAF SIP-TLS . 192.168.60.0/24 2001:DB8:1:60::/64 IPv4 IPv6 192.168.100.1(2001:DB8:1:100::1) .

.tACL : .

```
! !-- Include explicit permit statements for trusted sources !-- that require
access on the vulnerable protocols and ports ! access-list tACL-Policy
extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5060
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061 access-list tACL-Policy extended permit udp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy
extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5050 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 5620 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks ! access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended deny tcp
any 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy extended deny
udp any 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy extended
deny udp any 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy
extended deny tcp any 192.168.60.0 255.255.255.0 eq 5050 access-list tACL-
Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 5620 ! !-- Permit
or deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing
security policies and configurations ! !-- Explicit deny for all other IP
traffic ! access-list tACL-Policy extended deny ip any any ! !-- Include
explicit permit statements for trusted sources !-- that require access on the
vulnerable protocols and ports ! ipv6 access-list IPv6-tACL-Policy permit tcp
host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-
Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5061 ipv6
access-list IPv6-tACL-Policy permit udp host 2001:DB8:1:100::1
2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy permit udp host
2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-
Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5050 ipv6
access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1
2001:db8:1:60::/64 eq 5620 ! !-- The following vulnerability-specific access
control entries !-- (ACEs) can aid in identification of attacks ! ipv6
access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5060 ipv6
access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5061 ipv6
access-list IPv6-tACL-Policy deny udp any 2001:db8:1:60::/64 eq 5060 ipv6
access-list IPv6-tACL-Policy deny udp any 2001:db8:1:60::/64 eq 5061 ipv6
access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5050 ipv6
access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5620 ! !--
Permit/deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations ! !-- Explicit deny for all
other IP traffic ! ipv6 access-list IPv6-Transit-ACL-Policy deny ip any any
! !-- Apply tACLs to interfaces in the ingress direction ! access-group tACL-
Policy in interface outside access-group IPv6-Transit-ACL-Policy in interface
outside
```

: IP . RPF . RPF IP . IP RPF RPF . 3 RPF . RPF Cisco Security Appliance Command Reference for ip verify reverse-path Understanding Unicast Reverse Path Forwarding Applied Intelligence .: **TCP** TCP . , , . TCP . . TCP Cisco ASA 5500 Series Adaptive Security Appliance 7.0(1), 3.1(1) .TCP . TCP .TCP Cisco Unified Communications Manager TCP DoS . Cisco Unified Communications Manager . Cisco Unified Communications Manager TCP Cisco Unified Communications Manager .: . . 192.168.60.200/24 IP . TCP 1000 30 . . .

```
! !-- Match TCP traffic to the Cisco Unified Communications Manager ! access-
list CVE-2011-2560-acl extended permit tcp any host 192.168.60.200 class-map
CVE-2011-2560-cm match access-list CVE-2011-2560-acl ! !-- Configure the
connection limits for TCP !-- traffic to the Cisco Unified Communications
Manager ! policy-map global_policy class CVE-2011-2560-cm set connection
conn-max 1000 set connection timeout idle 0:30:00 service-policy
```

```
global_policy global
```

TCP CLI 8.2 Cisco ASA 5500 Series TCP .: tACL **show access-list** TCP UDP 5060 5061 SIP SIP-TLS . . show access-**list tACL-Policy** .

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 9 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq sip (hitcnt=34)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=24)
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq sip (hitcnt=4)
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=2)
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq sip (hitcnt=44)
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=61)
access-list tACL-Policy line 7 extended deny tcp any
     192.168.60.0 255.255.255.0 eq sip (hitcnt=5)
access-list tACL-Policy line 8 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=2)
access-list tACL-Policy line 9 extended deny udp any
     192.168.60.0 255.255.255.0 eq sip (hitcnt=7)
access-list tACL-Policy line 10 extended deny udp any
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=4)
access-list tACL-Policy line 11 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5050 (hitcnt=6)
access-list tACL-Policy line 12 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5620 (hitcnt=1)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=8)
firewall#
```

tACL-*Policy* .

- ACE 7 **TCP 5060 SIP 5**
- ACE 8 **TCP 5061 2 SIP-TLS**
- ACE 9 UDP **5060 SIP 7**
- ACE 10 UDP **5061 SIP 4**
- ACE 11 **TCP 5050 6 SAF**
- ACE 12 **TCP 5620** SAF **1**

IPv6 tACL , .: **Syslog** log ACE(Access Control Entry) syslog **106023** . syslog Cisco ASA 5500 Series System Log Message, 8.2 - 106023 .Cisco ASA 5500 Series Adaptive Security Appliance syslog Monitoring - Configuring Logging . Cisco Catalyst 6500 Series Cisco 7600 Series FWSM syslog Monitoring the Firewall Services Module . **show logging | grep** *regex* syslog . . **grep** . .

```
firewall#show logging | grep 106023
  Aug 28 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2924
         dst inside:192.168.60.191/sip by access-group "tACL-Policy"
  Aug 28 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/5061 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.19/2934
         dst inside:192.168.60.191/sip by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/5061 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/3961
         dst inside:192.168.60.197/5050 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.201/2939
         dst inside:192.168.60.185/5620 by access-group "tACL-Policy"
```

```
firewall#
```
tACL tACL **TCP UDP 5060 5061 SIP SIP-TLS** .ASA syslog Cisco ASA 5500 Series System Log Messages, 8.2 . FWSM syslog Catalyst 6500 Series Switch Cisco 7600 Series Router Firewall Services Module Logging System Log Messages .syslog Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence .: RPF syslog 106021 . syslog Cisco ASA 5500 Series System Log Message, 8.2 - 106021 .Cisco ASA 5500 Series Adaptive Security Appliance syslog Monitoring - Configuring Logging . Cisco Catalyst 6500 Series Cisco 7600 Series FWSM syslog Monitoring the Firewall Services Module . **show logging | grep** *regex* syslog . . **grep** . .

```
firewall#show logging | grep 106021
  Aug 24 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Aug 24 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Aug 24 2010 00:15:13: %ASA-1-106021: Deny TCP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
```

show asp drop RPF .

```
firewall#show asp drop frame rpf-violated
  Reverse-path verify failed                      11
firewall#
```

Unicast RPF Unicast RPF **11 IP** . RPF . Cisco Security Appliance Command Reference for show asp drop .**ID: TCP** Cisco ASA 5500 Series Adaptive Security Appliance **show service-policy** TCP .

```
firewall# show service-policy set connection detail

Global policy:
  Service-policy: global_policy
    Class-map: CVE-2011-2560-cm
      Set connection policy: conn-max 1000
        current conns 15, drop 5
      Set connection timeout policy:
        idle 0:30:00
        DCD: disabled, retry-interval 0:00:15, max-retries 5
        DCD: client-probe 0, server-probe 0, conn-expiration 0          11
firewall#
```

TCP **5** .**Cisco ACE: TCP** TCP Cisco ACE 4 , . TCP . ACE TCP TCP . ACE .TCP . TCP . .TCP Cisco Unified Communications Manager TCP , DoS . Cisco Unified Communications Manager . Cisco Unified Communications Manager TCP Cisco Unified Communications Manager .: . . 192.168.60.200/24 IP . TCP 1000 , 100000 , 30 .

```
! !-- Create a connection parameter map to group together TCP/IP !--
normalization and termination parameters ! parameter-map type connection CVE-
2011-2560-parameter-map limit-resource conc-connections 1000 set timeout
inactivity 1800 rate-limit connection 100000 ! !-- Match TCP traffic to the
Cisco Unified Communications Manager ! class-map match-any CVE-2011-2560-cm
match destination-address 192.168.60.200 ! !-- Configure the connection
limits for TCP !-- traffic to the Cisco Unified Communications Manager !
policy-map multi-match CVE-2011-2560_policy class CVE-2011-2560-cm connection
advanced-options CVE-2011-2560-parameter-map ! !-- Apply the policy to the
interface ! interface vlan 50 service-policy input CVE-2011-2560_policy
```

TCP Cisco ACE 4700 Series Appliance Security Configuration Guide Configuring TCP/IP Normalization and IP Reassembly Parameters .**ID: TCP** Cisco ACE Application Control Engine show .**Cisco : Cisco IPS** Cisco IPS(Intrusion Prevention System) . Cisco IPS 6.x S590 38386/0(: Cisco Intercompany Media Engine Denial of Service) . 38386/0 SFR(Signature Fidelity Rating) 15 Produce Alert . 38386/0 TCP 5620 . . Cisco IPS . . IP .Cisco IPS . Automatic Threat Prevention for Cisco IPS 6.x . riskRatingValue 90 . : IPS .**Cisco , :** **Cisco ,** Cisco Security MARS(Monitoring, Analysis, and Response System) IPS 38386/0(: Cisco Intercompany Media Engine Denial Of Service) . S590 IPS 38386/0 **NR-38386/0 < All Matching Events** Cisco Security MARS Appliance **| All Matching Event Raw Messages( )>** IPS .Cisco Security MARS 4.3.1 5.3.1 Cisco IPS . Cisco.com , , . MARS IPS .: . MARS . . Cisco MARS .

```
System Rule: CS-MARS IPS Signature Update Failure
```

> *IPS* MARS . Cisco Security MARS 4.3.1 5.3.1 .

추가 정보

이 문서는 "있는 그대로" 제공되며, 상품성 또는 특정 사용에 대한 적합성의 보증을 포함하여 어떤 종류의 보장 또는 보증도 의미하지 않습니다. 문서 또는 문서에 링크된 자료의 정보를 사용하는 것은 귀하의 책임입니다. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

개정 이력

개정 1.1	2011년 11월 2일	수정된 문서 URL
개정 1.0	2011년 8월 24일	초기 공개

Cisco 보안 절차

Cisco 제품의 보안 취약성 보고, 보안 사고에 대한 지원 요청, Cisco의 보안 정보 수신을 위한 등록 등에 대한 자세한 내용은 Cisco의 전 세계 웹 사이트 (https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html)에서 확인할 수 있습니다. 여기에는 Cisco 보안 알림과 관련된 언론 문의에 대한 지침이 포함됩니다. 모든 Cisco 보안 권고 사항은 http://www.cisco.com/go/psirt에서 확인할 수 있습니다.

관련 정보

- Cisco Applied Mitigation 게시판
- Cisco 보안
- Cisco Security IntelliShield Alert Manager Service
- Cisco IOS 디바이스를 강화하는 Cisco 가이드
- Cisco IOS NetFlow - 홈 페이지(Cisco.com)
- Cisco IOS NetFlow 백서
- NetFlow 성능 분석
- Cisco 네트워크 기반 보호 백서
- Cisco 방화벽 제품 - 홈 페이지 Cisco.com
- Cisco ACE Application Control Engine 모듈 설명서
- 인터넷 서비스 공급자를 위한 유니캐스트 역방향 경로 전달 개선 사항
- Cisco 침입 방지 시스템
- Cisco IPS 서명 다운로드
- Cisco IPS 서명 검색 페이지
- Cisco 보안 모니터링, 분석 및 대응 시스템
- CVE(Common Vulnerabilities and Exposures)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.