Identifizieren und Vermindern der Ausnutzung der Überlaufschwachstelle des PHP HTML Entity Encoder-Heaps in mehreren webbasierten Managementschnittstellen

Identifizieren und Vermindern der Ausnutzung der Überlaufschwachstelle des PHP HTML Entity Encoder-Heaps in mehreren webbasierten Managementschnittstellen

Beratungs-ID: cisco-amb-20070425-http

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070425-http

Version 1.0

Zur öffentlichen Veröffentlichung 2007 April 25 16:00 UTC (GMT)

Inhalt

Antwort von Cisco

Dieses Applied Mitigation Bulletin ist ein Begleitdokument zur PSIRT Security Response: PHP HTML Entity Encoder Heap Overflow Vulnerability in Multiple Web-Based Management Interfaces. Er dokumentiert zusätzliche Eindämmungstechniken, die auf Cisco Geräten im Netzwerk implementiert werden können.

Merkmale der Schwachstelle

In bestimmten PHP-Funktionen, die zu bestimmten Cisco Produkten gehören, besteht eine Schwachstelle. Ein authentifizierter Angreifer kann diese Sicherheitslücke aus der Ferne ausnutzen. Eine Benutzerinteraktion ist nicht erforderlich. Wenn diese Schwachstelle erfolgreich

ausgenutzt wird, kann möglicherweise nicht privilegierter Code ausgeführt werden. Die Vektoren, die zur Ausnutzung dieser Schwachstelle verwendet werden, sind die HTTP- und HTTPS-Protokolle (TCP-Ports 80 und 443). Diese Verwundbarkeit wird durch die CVE-ID 2006-5465 abgedeckt.

Informationen zu anfälliger, nicht betroffener und fester Software finden Sie in der PSIRT-Sicherheitsantwort unter https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070425-http

Überblick über die Risikominderungstechnik

Cisco-Geräte bieten verschiedene Gegenmaßnahmen für die Überlaufschwachstelle des PHP-HTML-Encoders. Viele dieser Schutzmethoden sollten als allgemeine Best Practices für die Sicherheit von Infrastrukturgeräten und des Datenverkehrs betrachtet werden, der durch das Netzwerk fließt.

Die Cisco IOS Software bietet mithilfe von Infrastruktur-Zugriffskontrolllisten (Infrastructure Access Control Lists, iACLs) effektive Möglichkeiten zur Verhinderung von Exploits. Cisco ASA-, PIX- und Firewall Services Module (FWSM)-Firewalls bieten darüber hinaus effektive Möglichkeiten zur Verhinderung von Exploits mithilfe von Transit-Zugriffskontrolllisten (Transit Access Control Lists, tACLs). Sowohl Infrastruktur- als auch Transit-Zugriffskontrolllisten (ACLs) filtern die Quell-IP-Adresse von Paketen, die versuchen, die in diesem Dokument beschriebene Schwachstelle auszunutzen, und verwerfen sie.

Die Cisco IOS NetFlow-Funktion steuert Datenströme mithilfe von Datenflussaufzeichnungen und Cisco IOS Software, Cisco Adaptive Security Appliances der Serie ASA 5500, Cisco PIX 500 Security Appliances sowie FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 über Syslog-Meldungen und die Zählerwerte, die in der Ausgabe von show-Befehle.

Risikomanagement

Unternehmen sollten den üblichen Prozess zur Risikominimierung einhalten, um die potenziellen Auswirkungen dieser Schwachstelle zu ermitteln. Dokumente, die für die Risikoeinschätzung verwendet werden können, sind unter Risikoeinschätzung für Ankündigungen von Sicherheitslücken und Risikoeinschätzung und Prototyping verfügbar.

Gerätespezifische Eindämmung und Identifizierung

Vorsicht: Die Effektivität der Risikominimierungstechnik hängt von spezifischen Kundensituationen wie Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischem Auftrag ab. Prüfen Sie wie bei jeder Konfigurationsänderung die Auswirkungen dieser Konfiguration, bevor Sie die Änderung übernehmen.

Spezifische Informationen zur Risikominderung und Identifizierung sind für die folgenden Geräte verfügbar:

- Cisco IOS-Router
- Cisco IOS-NetFlow

- Cisco ASA, PIX und FWSM-Firewalls

Cisco IOS-Router

Eindämmung: Infrastruktur-Zugriffskontrolllisten

Um Infrastrukturgeräte zu schützen und das Risiko, die Auswirkungen und die Effektivität direkter Angriffe auf die Infrastruktur zu minimieren, sollten Infrastruktur-Zugriffskontrolllisten (iACLs) bereitgestellt werden, um die Richtliniendurchsetzung für den an Infrastrukturgeräte gesendeten Datenverkehr durchzuführen. Administratoren können eine iACL erstellen, indem sie explizit zulassen, dass nur autorisierter Datenverkehr gemäß den bestehenden Sicherheitsrichtlinien und -konfigurationen an die Geräte der Infrastruktur gesendet wird. Für einen maximalen Schutz von Infrastrukturgeräten sollten iACLs in Eingangsrichtung auf alle Schnittstellen angewendet werden, auf denen eine Layer-3-IP-Adresse konfiguriert wurde.

Im folgenden Beispiel ist der Adressblock 192.168.1.0/24 der Infrastruktur-Adressraum. Die iACL-Richtlinie verweigert HTTP- und HTTPS-Pakete, die an die TCP-Ports 80 und 443 gerichtet und an Adressen gesendet werden, die Teil des Infrastruktur-Adressbereichs sind. Es sollte darauf geachtet werden, dass der erforderliche Datenverkehr für das Routing und den Administratorzugriff zugelassen wird, bevor der gesamte Datenverkehr abgelehnt wird, der direkt an Infrastrukturgeräte gesendet wird. Wenn möglich, sollte sich der Infrastruktur-Adressraum vom Adressraum unterscheiden, der für Benutzer- und Service-Segmente verwendet wird. Mit dieser Adressierungsmethode können Sie iACLs erstellen und bereitstellen.

Zusätzliche Zugriffskontrolleinträge (ACEs) sollten als Teil einer iACL-Richtlinie implementiert werden, die zum Filtern des Datenverkehrs an den Netzwerkeingangspunkten verwendet wird.

Weitere Informationen zu iACLs finden Sie unter Protecting Your Core: Infrastructure Protection Access Control Lists (Schützen Ihres Kerns: Zugriffskontrolllisten für Infrastrukturschutz).

```
ip access-list extended infrastructure-acl-policy
!-- Permit additional Layer 3 and Layer 4 traffic destined for infrastructure !--
address space as dictated by existing security policies and configurations. ! !--
Permit/deny traffic to infrastructure IP addresses in accordance !-- with security
policy. ! !-- Vulnerability-specific deny statements to aid identification deny tcp
any 192.168.1.0 0.0.0.255 eq 80 deny tcp any 192.168.1.0 0.0.0.255 eq 443 !-- Default
deny to affected IP addresses deny ip any 192.168.1.0 0.0.0.255 !-- Permit/deny all
other IP traffic in accordance with !-- existing security policies and
configurations. ! !-- Apply iACL to interface(s) in the ingress direction. interface
GigabitEthernet0/0 ip access-group infrastructure-acl-policy in !
```

Beachten Sie, dass das Filtern mit einer Schnittstellenzugriffsliste die Übertragung von nicht erreichbaren ICMP-Nachrichten zurück an die Quelle des gefilterten Datenverkehrs auslöst. Dies könnte den unerwünschten Effekt einer erhöhten CPU-Auslastung haben, da das Filtergerät diese nicht erreichbaren ICMP-Meldungen generieren muss. In IOS ist die Erzeugung von "ICMP unreachable" (nicht erreichbar) auf ein Paket alle 500 Millisekunden beschränkt. Die Erzeugung von nicht erreichbaren ICMP-Nachrichten kann mit dem Schnittstellenkonfigurationsbefehl **no icmp unreachables** deaktiviert werden. Die Durchsatzbegrenzung "ICMP Unreachable" kann mit dem globalen Konfigurationsbefehl **ip icmp rate-limit unreachable** *interval-in-ms* standardmäßig von 1 pro 500 Millisekunden geändert werden. Administratoren können Intervalle zwischen 1 und 4294967295 Millisekunden angeben.

Identifikation: Infrastruktur-Zugriffskontrolllisten

Bei einer iACL kann nach Anwendung der Zugriffsliste auf eine Schnittstelle in Eingangsrichtung mit dem Befehl **show access-list** die Anzahl der HTTP- und HTTPS-Pakete auf den TCP-Ports 80 und 443 identifiziert werden, die gefiltert werden. Gefilterte Pakete sollten untersucht werden, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen. Beispielausgabe für **show access-list infrastructure-acl-policy**:

```
router#show access-list infrastructure-acl-policy
Extended IP access list infrastructure-acl-policy
10 deny tcp any 192.168.1.0 0.0.0.255 eq 80 (92 matches)
20 deny udp any 192.168.1.0 0.0.0.255 eq 443 (23 matches)
30 deny ip any 192.168.1.0 0.0.0.255
-- Infrastructure ACL Policy Truncated --
router#
```

Im vorherigen Beispiel hat die Zugriffslisten-*infrastruktur-acl-policy* 92 HTTP-Pakete auf dem TCP-Port 80 für die ACE-Sequenz-ID 10 und 23 HTTPS-Pakete auf dem TCP-Port 443 für die ACE-Sequenz-ID 20 verworfen. Diese iACL wird in Eingangsrichtung auf die GigabitEthernet0/0-Schnittstelle angewendet.

Cisco IOS-NetFlow

Identifizierung: Identifikation des Datenverkehrsflusses mithilfe von NetFlow-Datensätzen

Cisco IOS NetFlow kann auf Cisco IOS-Routern und -Switches konfiguriert werden, um Datenverkehrsflüsse zu identifizieren, die die in diesem Dokument beschriebene Schwachstelle ausnutzen könnten. Pakete sollten untersucht werden, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen, oder um legitimen Datenverkehr.

```
router#show ip cache flow
IP packet size distribution (149962503 total packets):
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.008 .582 .047 .008 .008 .008 .005 .012 .000 .001 .004 .001 .002 .002 .006
512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.001 .001 .161 .011 .122 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
27 active, 65509 inactive, 65326701 added
208920154 ager polls, 0 flow alloc failures
Active flows timeout in 1 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
27 active, 16357 inactive, 4854213 added, 4854213 added to flow
0 alloc failures, 0 force free
1 chunk, 11 chunks 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 11409641 2.6 1 49 3.1 0.0 1.5
TCP-FTP 7371 0.0 8 54 0.0 6.0 7.8
TCP-FTPD 713 0.0 3109 889 0.5 50.4 0.6
TCP-WWW 182891 0.0 13 735 0.5 4.3 9.3
TCP-SMTP 12 0.0 1 47 0.0 0.0 10.5
TCP-X 731 0.0 1 40 0.0 0.0 1.4
TCP-BGP 13 0.0 1 46 0.0 0.0 10.3
TCP-NNTP 12 0.0 1 47 0.0 0.0 9.7
TCP-Frag 70401 0.0 1 688 0.0 0.0 22.7
TCP-other 49417868 11.5 2 340 28.8 0.1 1.4
```

```
UDP-DNS 1411124 0.3 1 57 0.4 0.0 15.4
UDP-NTP 1365184 0.3 1 76 0.3 0.6 15.5
UDP-TFTP 10 0.0 2 57 0.0 6.6 18.6
UDP-other 1134163 0.2 2 160 0.5 0.3 16.6
ICMP 325667 0.0 7 48 0.5 11.7 20.0
IPv6INIP 15 0.0 1 1132 0.0 0.0 15.4
GRE 694 0.0 1 50 0.0 0.0 15.4
IP-other 2 0.0 2 20 0.0 0.1 15.7
Total: 65326512 15.2 2 315 34.9 0.1 2.4

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Gi0/0 10.21.96.74 Gi0/1* 192.168.1.11 06 F079 01BB 4
Gi0/0 10.21.96.74 Gi0/1 192.168.1.11 06 F079 01BB 4
Gi0/0 10.89.16.34 Gi0/1* 192.168.150.60 06 0FC8 0016 1
Gi0/0 10.89.16.34 Gi0/1 192.168.150.60 06 0FC8 0016 1
Gi0/1 192.168.150.60 Gi0/0* 10.89.16.34 06 0016 0FC8 1
Gi0/1 192.168.150.60 Gi0/0 10.89.16.34 06 0016 0FC8 1
Gi0/1 192.168.150.1 Gi0/0* 198.41.0.4 11 0401 0035 1
Gi0/1 192.168.150.1 Gi0/0 198.41.0.4 11 0401 0035 1
Gi0/0 192.168.208.63 Local 192.168.208.20 06 8876 0017 76
Gi0/1 192.168.128.2 Gi0/0* 10.88.226.1 11 007B 007B 1
Gi0/1 192.168.128.2 Gi0/0 10.88.226.1 11 007B 007B 1
Gi0/1 192.168.144.3 Gi0/0* 10.88.226.1 11 007B 007B 1
Gi0/1 192.168.144.3 Gi0/0 10.88.226.1 11 007B 007B 1
Gi0/0 10.88.226.1 Gi0/1* 192.168.144.3 11 007B 007B 1
Gi0/0 10.88.226.1 Gi0/1 192.168.144.3 11 007B 007B 1
Gi0/1 192.168.150.1 Gi0/0* 192.228.79.201 11 0401 0035 1
Gi0/1 192.168.150.1 Gi0/0 192.228.79.201 11 0401 0035 1
Gi0/1 192.168.150.1 Gi0/0* 128.63.2.53 11 0401 0035 1
Gi0/1 192.168.150.1 Gi0/0 128.63.2.53 11 0401 0035 1
```

Im vorherigen Beispiel gibt es mehrere Flows für das HTTPS-Protokoll auf Port 443 (Hex-Wert <01BB>). Dieser Datenverkehr stammt aus der Adresse 10.21.96.74 und wird an die Adresse 192.168.1.11 gesendet, die für Infrastrukturgeräte verwendet wird. Netzwerkadministratoren können **include-**Anweisungen verwenden, um nur bestimmte Ziel-IP-Adressen oder Ziel-Ports einzuschließen und so die NetFlow-Ausgabe auf Daten zu beschränken, die mit höherer Wahrscheinlichkeit relevant sind. Ein Beispiel wäre **show ip cache flow | 01BB einschließen**, d. h. nur Hosts anzeigen, für die der TCP-Port 443 (Hexadezimalwert <01BB>) verwendet wird. Diese Datenflüsse sollten untersucht werden, um festzustellen, ob sie von nicht vertrauenswürdigen Hosts und/oder Netzwerken stammen.

Cisco ASA, PIX und FWSM-Firewalls

Eindämmung: Transit-Zugriffskontrolllisten

Um das Netzwerk vor dem Edge-Datenverkehr zu schützen, der am Eingangspunkt in das Netzwerk gelangt, oder vor dem Datenverkehr, der das Netzwerk durchquert, sollten Zugriffskontrolllisten (tACLs) bereitgestellt werden, um die Richtlinien für diesen Datenverkehr durchzusetzen. Administratoren können eine tACL erstellen, indem sie explizit zulassen, dass nur autorisierter Datenverkehr an den Eingangs-Access Points in das Netzwerk eindringt, oder indem sie autorisiertem Datenverkehr gestatten, das Netzwerk gemäß den bestehenden Sicherheitsrichtlinien und -konfigurationen zu passieren.

Im folgenden Beispiel ist der Adressblock 192.168.1.0/24 der Infrastruktur-Adressraum. Die tACL-Richtlinie verweigert nicht autorisierte Pakete auf den TCP-Ports 80 (HTTP) und 443 (HTTPS), die an Adressen gesendet werden, die Teil des Infrastruktur-Adressbereichs sind.

Es sollte darauf geachtet werden, dass der für das Routing und den Administratorzugriff erforderliche Datenverkehr zugelassen wird, bevor nicht autorisierter Datenverkehr abgelehnt wird. Wenn möglich, sollte sich der Infrastruktur-Adressraum vom Adressraum unterscheiden, der für Benutzer- und Service-Segmente verwendet wird. Die Verwendung dieser Adressierungsmethode wird bei der Erstellung und Bereitstellung von tACLs helfen.

Weitere Informationen zu tACLs finden Sie unter Transit Access Control Lists: Filtering at Your Edge.

```
!-- Permit/Deny additional Layer 3 and Layer 4 traffic to enter !-- the network at
ingress access points or traffic that has been un/authorized !-- to transit the
network in accordance with existing security policies !-- and configurations. Deny
all !-- packets on TCP ports 80 and 443 sent to any IP address configured within the
!-- address block of 192.168.1.0/24, which is the infrastructure address !-- space,
except from known trusted source networks (ex: management networks, !-- security
operations center, network operations center). ! !-- The following are vulnerability-
specific access control entries (ACEs) to aid !-- in identification of attacks.
access-list transit-acl-policy extended deny tcp any 192.168.1.0 255.255.255.0 eq www
access-list transit-acl-policy extended deny tcp any 192.168.1.0 255.255.255.0 eq
https ! !-- Explicit default deny ACE for unauthorized traffic entering the network
!-- at ingress access points or unauthorized transit traffic sent to addresses !--
configured within the infrastructure address space. access-list transit-acl-policy
extended deny ip any 192.168.1.0 255.255.255.0 ! !-- Permit/Deny all other Layer 3
and Layer 4 traffic in accordance with !-- existing security policies and
configurations. ! !-- Apply tACL to interface(s) in the ingress direction. access-
group transit-acl-policy in interface outside !
```

Identifizierung: Transit-Zugriffskontrolllisten

Bei einer tACL kann nach Anwendung der Zugriffsliste auf eine Schnittstelle in Eingangsrichtung mit dem Befehl **show access-list** die Anzahl der HTTP- und HTTPS-Pakete auf den TCP-Ports 80 und 443 identifiziert werden, die gefiltert werden. Gefilterte Pakete sollten untersucht werden, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen. Ein Beispiel für die Ausgabe von **show access-list transit-acl-policy** ist:

```
firewall# show access-list transit-acl-policy
access-list transit-acl-policy line 1 extended deny tcp any 192.168.1.0 255.255.255.0
eq www (hitcnt=11)
access-list transit-acl-policy line 2 extended deny tcp any 192.168.1.0 255.255.255.0
eq https (hitcnt=6)
access-list transit-acl-policy line 3 extended deny ip any 192.168.1.0 255.255.255.0
(hitcnt=0)

-- Transit ACL Policy Truncated --
firewall#
```

Im vorherigen Beispiel hat die Zugriffsliste "*transit-acl-policy*" 11 HTTP-Pakete verworfen, die für TCP-Port 80 bestimmt sind, sowie sechs HTTPS-Pakete, die für TCP-Port 443 bestimmt sind und von nicht vertrauenswürdigen Hosts oder Netzwerken empfangen wurden. Diese tACL wird auf die Schnittstelle *außerhalb* in Eingangsrichtung angewendet.

Identifizierung: Firewall-Syslog-Meldungen

Die Firewall-Syslog-Meldung 106023 wird für Pakete generiert, die von einem ACE abgelehnt wurden, der nicht über das **log**-Schlüsselwort verfügt. Weitere Informationen zu dieser Syslog-Meldung finden Sie unter Cisco Security Appliance System Log Message - 106023.

Informationen zur Konfiguration von Syslog für die Cisco Adaptive Security Appliance der Serie ASA 5500 oder die Cisco Security Appliance der Serie PIX 500 finden Sie unter Configuring Logging (Konfigurieren der Protokollierung) auf der Cisco Security Appliance. Informationen zur Konfiguration von Syslog auf dem FWSM für Cisco Catalyst Switches der Serie 6500 und Cisco Router der Serie 7600 finden Sie unter Configuring Logging (Konfigurieren der Protokollierung) auf der Cisco Security Appliance.

In den folgenden Beispielen **zeigt** die **Protokollierung | grep regex** wird verwendet, um Syslog-Meldungen aus dem Protokollierungspuffer der Firewall zu extrahieren. Auf diese Weise werden zusätzliche Informationen über abgelehnte Pakete abgerufen, die auf potenzielle Versuche hinweisen könnten, die in diesem Dokument beschriebene Schwachstelle auszunutzen. Es ist möglich, verschiedene Regex-Muster mit dem **grep**-Schlüsselwort zu verwenden, um nach bestimmten Daten zu suchen, die innerhalb der protokollierten Nachrichten vorhanden sind. In einigen Fällen ist es möglich, schädlichen Datenverkehr mithilfe mehrerer **grep**-Befehle und regulärer Ausdrücke schneller zu identifizieren.

```
firewall#show logging | grep 106023
Apr 11 2007 14:31:17: %ASA-4-106023: Deny tcp src outside:192.168.208.63/34938 dst
inside:192.168.1.5/80 by access-group "transit-acl-policy" [0x55c1c7ff, 0x0]
Apr 11 2007 14:31:18: %ASA-4-106023: Deny tcp src outside:192.168.208.63/34939 dst
inside:192.168.1.5/80 by access-group "transit-acl-policy" [0x55c1c7ff, 0x0]
Apr 11 2007 14:31:25: %ASA-4-106023: Deny tcp src outside:192.168.208.63/34940 dst
inside:192.168.1.6/80 by access-group "transit-acl-policy" [0x55c1c7ff, 0x0]
```

Im vorherigen Beispiel zeigen die für die tACL *transit-acl-policy* protokollierten Meldungen (106023) HTTP- und HTTPS-Pakete für die TCP-Ports 80 und 443 an, die an den der Netzwerkinfrastruktur zugewiesenen Adressblock gesendet wurden. Wenn Administratoren schädliche Quelladressen identifizieren, möchten sie möglicherweise **grep**-Befehle mit den zugehörigen schädlichen IP-Adressen verwenden, um festzustellen, ob andere Versuche unternommen wurden. Es ist möglicherweise ratsam, gespeicherte Protokolldaten zu recherchieren, um festzustellen, welche anderen Aktivitäten mit den schädlichen IP-Adressen verbunden sind.

Weitere Informationen zu Syslog-Meldungen für ASA- und PIX-Sicherheits-Appliances finden Sie unter Cisco Security Appliance System Log Messages. Weitere Informationen zu Syslog-Meldungen für FWSM finden Sie unter Catalyst Switch der Serie 6500 und Cisco Router der Serie 7600 Firewall Services Module Logging Configuration (Protokollierungskonfiguration für das Firewall-Servicemodul) und System Log Messages (Systemprotokollmeldungen).

Zusätzliche Informationen

Revisionsverlauf

Version 1.0	25. April 2007	Erste öffentliche Veröffentlichung

Cisco Sicherheitsverfahren

Vollständige Informationen zur Meldung von Sicherheitslücken in Cisco Produkten, zum Erhalt von Unterstützung bei Sicherheitsvorfällen und zur Registrierung für den Erhalt von Sicherheitsinformationen von Cisco finden Sie auf der weltweiten Cisco Website unter https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dies beinhaltet Anweisungen für Presseanfragen bezüglich der Sicherheitshinweise von Cisco. Alle Cisco Sicherheitsankündigungen finden Sie unter http://www.cisco.com/go/psirt.

Zugehörige Informationen

- Protecting Your Core: Infrastructure Protection - Zugriffskontrolllisten
- Transit-Zugriffskontrolllisten: Filterung am Netzwerk-Edge
- Cisco IOS NetFlow - Startseite auf Cisco.com
- Cisco IOS NetFlow-Whitepaper
- Cisco Network Foundation Protection - Whitepaper
- Cisco Network Foundation Protection - Präsentationen
- Cisco Firewall-Produkte - Startseite auf Cisco.com

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.