



Hardwareinstallationshandbuch für Cisco Secure Firewall der 6100-Serie

Letzte Änderung: 21. April 2026

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

DIE SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN PRODUKTEN IN DIESEM HANDBUCH KÖNNEN OHNE VORHERIGE ANKÜNDIGUNG GEÄNDERT WERDEN. ALLE ANGABEN, INFORMATIONEN UND EMPFEHLUNGEN IN DIESEM HANDBUCH WURDEN IN DER ANNAHME ZUR VERFÜGUNG GESTELLT, DASS SIE KORREKT SIND. JEDE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG IST JEDOCH AUSGESCHLOSSEN. DIE ALLEINIGE VERANTWORTUNG FÜR DIE ANWENDUNG DER PRODUKTE LIEGT BEI DEN BENUTZERN.

DIE SOFTWARELIZENZ UND BESCHRÄNKTE GEWÄHRLEISTUNG FÜR DAS BEILIEGENDE PRODUKT SIND IM INFORMATIONSPAKET FÜR DAS PRODUKT ENTHALTEN UND WERDEN DURCH DIESE BEZUGNAHME IN DIE VORLIEGENDEN BESTIMMUNGEN EINGESCHLOSSEN. WENN SIE DIE SOFTWARELIZENZ ODER BESCHRÄNKTE GARANTIE NICHT FINDEN KÖNNEN, WENDEN SIE SICH AN EINEN VERTRETER VON CISCO, UM EINE KOPIE ZU ERHALTEN.

Die folgenden Informationen beziehen sich auf die Einhaltung der FCC-Richtlinien für Geräte der Klasse A: Dieses Gerät wurde getestet und erfüllt die Grenzwerte für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Richtlinien. Diese Anforderungen ermöglichen einen angemessenen Schutz gegen elektromagnetische Störungen, wenn das Gerät in einem gewerblichen Umfeld eingesetzt wird. Dieses Gerät erzeugt und verwendet Hochfrequenzsignale und kann diese abstrahlen. Wenn dieses Gerät nicht gemäß der Bedienungsanleitung installiert und betrieben wird, kann es Funkstörungen verursachen. Der Betrieb dieses Geräts in einem Wohngebiet kann unter Umständen zu funktechnischen Störungen führen. In diesem Fall muss der Benutzer diese Störungen auf eigene Kosten beheben.

Die folgenden Informationen betreffen FCC-konforme Geräte der Klasse B: Dieses Gerät wurde getestet und erfüllt die Anforderungen für digitale Geräte der Klasse B gemäß Abschnitt 15 der FCC-Bestimmungen. Diese Anforderungen ermöglichen einen angemessenen Schutz gegen elektromagnetische Störungen im häuslichen Bereich. Dieses Gerät erzeugt und verwendet Hochfrequenzsignale und kann diese abstrahlen. Wenn dieses Gerät nicht gemäß den Anweisungen installiert und betrieben wird, kann es Funkstörungen verursachen. Es kann jedoch nicht in jedem Fall garantiert werden, dass bei ordnungsgemäßer Installation keine Störungen auftreten. Wenn das Gerät Störungen beim Rundfunk- oder Fernsehempfang verursacht, was sich durch Aus- und Wiedereinschalten des Gerätes überprüfen lässt, versuchen Sie, die Störung durch eine der folgenden Maßnahmen zu beheben:

- Verändern Sie die Ausrichtung oder den Standort der Empfangsantenne.
- Erhöhen Sie den Abstand zwischen dem Gerät und dem Empfänger.
- Schließen Sie das Gerät an einen anderen Hausstromkreis an als den Empfänger.
- Wenden Sie sich an den Händler oder einen erfahrenen Radio-/Fernsehtechniker.

Anpassungen und Veränderungen an diesem Produkt, die nicht durch Cisco autorisiert wurden, können die FCC-Genehmigung außer Kraft setzen und zum Verlust der Erlaubnis führen, dieses Produkt zu betreiben.

Die Cisco Implementierung der TCP-Headerkomprimierung ist eine Adaption eines Programms, das an der University of California, Berkeley (UCB) als Teil der Public-Domain-Version der UCB für das UNIX-Betriebssystem entwickelt wurde. Alle Rechte vorbehalten. Copyright © 1981, Regents of the University of California, USA.

UNGEACHTET SONSTIGER GEWÄHRLEISTUNGEN WERDEN ALLE DOKUMENT- UND SOFTWAREDATEIEN DIESER ANBIETER WIE VORLIEGEND OHNE MÄNGELGEWÄHRBEREITGESTELLT. CISCO UND ALLE ZUVOR GENANNTE LIEFERANTEN ÜBERNEHMEN KEINERLEI, AUSDRÜCKLICHE ODER STILLSCHWEIGENDE, GARANTIE, EINSCHLIEBLICH UND OHNE EINSCHRÄNKUNG, DIEJENIGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG ODER DIEJENIGEN, DIE AUS DEM VERLAUF DES HANDELNS, DER VERWENDUNG ODER DES HANDELSBRAUCHS ENTSTEHEN.

UNTER KEINEN UMSTÄNDEN HAFTEN CISCO ODER SEINE ZULIEFERER FÜR JEDLICHE INDIREKTEN, KONKRETE, ZUFÄLLIGEN ODER FOLGESCHÄDEN, DARUNTER BEISPIELSWEISE ENTGANGENE GEWINNE ODER DATENVERLUSTE, DIE AUS DER VERWENDUNG ODER NICHTVERWENDBARKEIT DIESER HANDBUCHS ERWACHSEN, SELBST FÜR DEN FALL, DASS CISCO ODER SEINE ZULIEFERER AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDEN.

Alle in diesem Dokument verwendeten IP-Adressen (Internet Protocol) und Telefonnummern sind als Beispiele zu verstehen und beziehen sich nicht auf tatsächlich existierende Adressen und Telefonnummern. Die in diesem Dokument enthaltenen Beispiele, Befehlsausgaben, Netzwerktopologie-Diagramme und andere Abbildungen dienen lediglich zur Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen oder Telefonnummern in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

Für gedruckte und kodierte digitale Versionen dieses Dokuments besteht keine Gewährleistung. Die aktuelle Online-Version enthält die neueste Version.

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen und Telefonnummern finden Sie auf der Cisco Website unter www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. Alle Rechte vorbehalten.



INHALTSVERZEICHNIS

KAPITEL 1

Überblick 1

Merkmale	1
Lieferumfang	4
Seriennummer und QR-Code für das Dokumentationsportal	6
Vorderseite	8
Power-Taste und Reset-Taste	9
Management-Port, Konsolen-Port und USB-Port	11
LEDs an der Vorderseite	12
Rückseite	14
1/10/25-Gbit/s-Netzwerkmodul mit 8 Ports (CSF6K-XNM-8X10G)	15
40-Gbit/s-Netzwerkmodul mit 4 Ports(CSF6K-XNM-4X40G)	17
2-Port-Netzwerkmodul mit 100 Gbit/s(CSF6K-XNM-2X100G)	18
200-Gbit/s--Netzwerkmodul mit 4 Ports(CSF6K-XNM-4X200G)	20
400-Gbit/s-Netzwerkmodul mit 2 Ports(CSF6K-XNM-2X400G)	22
1000Base-T-Netzwerkmodul mit Hardwareumgehung und 8 Ports (CSF6K-XNM-8X1GF)	24
6-Port-Netzwerkmodul mit 1 Gbit/s SX/10-Gbit/s SR/10-Gbit/s LR/25-Gbit/s SR/25-Gbit/s LR mit Hardware-Umgehung (CSF6K-XNM-6X10SRF, CSF6K-XNM-6X10LRF, CSF6K-XNM-6X25SRF und CSF6K-XNM-6X25LRF)	26
Netzstrommodule	29
Lüftermodule	31
SSDs	32
Unterstützte Transceiver	33
Hardwarespezifikationen	49
Produkt-IDs	50
Netzkabelspezifikationen	53

KAPITEL 2

Vorbereitung der Installation 71

Warnhinweise für die Installation	71
Sicherheitshinweise	73
Sicherheit bei Arbeiten mit Elektrizität	74
Vermeidung von Schäden durch ESD	74
Standortumgebung	75
Standortbezogene Überlegungen	75
Überlegungen zur Stromversorgung	75
Überlegungen zur Rack-Konfiguration	76

KAPITEL 3**Montage des Chassis 77**

Auspacken und Prüfen des Chassis	77
Rackmontage des Chassis mit Gleitschienen	78
Erdung des Chassis	85

KAPITEL 4**Installation, Wartung und Upgrade 89**

Installieren, Entfernen und Austauschen des Netzwerkmoduls	89
Entfernen und Austauschen der SSD	91
Entfernen und Austauschen des Lüftermoduls	92
Entfernen und Austauschen des Netzteilmoduls	94
Entfernen und Austauschen von DIMMs	96



KAPITEL 1

Überblick

- Merkmale, auf Seite 1
- Lieferumfang, auf Seite 4
- Seriennummer und QR-Code für das Dokumentationsportal, auf Seite 6
- Vorderseite, auf Seite 8
- Power-Taste und Reset-Taste, auf Seite 9
- Management-Port, Konsolen-Port und USB-Port, auf Seite 11
- LEDs an der Vorderseite, auf Seite 12
- Rückseite, auf Seite 14
- 1/10/25-Gbit/s-Netzwerkmodul mit 8 Ports (CSF6K-XNM-8X10G), auf Seite 15
- 40-Gbit/s-Netzwerkmodul mit 4 Ports(CSF6K-XNM-4X40G), auf Seite 17
- 2-Port-Netzwerkmodul mit 100 Gbit/s(CSF6K-XNM-2X100G), auf Seite 18
- 200-Gbit/s-Netzwerkmodul mit 4 Ports(CSF6K-XNM-4X200G), auf Seite 20
- 400-Gbit/s-Netzwerkmodul mit 2 Ports(CSF6K-XNM-2X400G), auf Seite 22
- 1000Base-T-Netzwerkmodul mit Hardwareumgehung und 8 Ports (CSF6K-XNM-8X1GF), auf Seite 24
- 6-Port-Netzwerkmodul mit 1 Gbit/s SX/10-Gbit/s SR/10-Gbit/s LR/25-Gbit/s SR/25-Gbit/s LR mit Hardware-Umgehung (CSF6K-XNM-6X10SRF, CSF6K-XNM-6X10LRF, CSF6K-XNM-6X25SRF und CSF6K-XNM-6X25LRF), auf Seite 26
- Netzstrommodule, auf Seite 29
- Lüftermodule, auf Seite 31
- SSDs, auf Seite 32
- Unterstützte Transceiver, auf Seite 33
- Hardwarespezifikationen, auf Seite 49
- Produkt-IDs, auf Seite 50
- Netzkabelspezifikationen, auf Seite 53

Merkmale

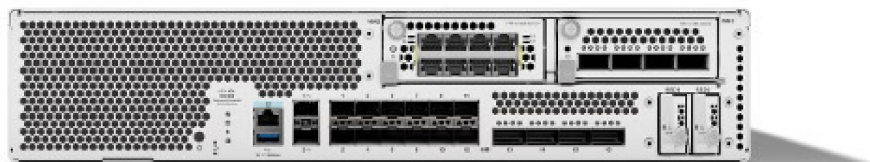
Die Secure Firewall der Cisco 6100-Serie ist eine eigenständige modulare Plattform für Sicherheitservices, die die Modelle 6160 und 6170 umfasst. Unter [Produkt-IDs, auf Seite 50](#) finden Sie eine Liste der Produkt-IDs (PIDs) für die Serie 6100.

Die Secure Firewall 6100-Serie unterstützt Cisco Secure Firewall Threat Defense-Software Version 10.0.0 und Cisco Secure ASA-Software Version 9.24.1. Weitere Informationen finden Sie im [Cisco Secure Firewall](#)

[Threat Defense-Kompatibilitätsleitfaden](#) und im [Cisco Secure Firewall ASA-Kompatibilitätsleitfaden](#), die Informationen zur Kompatibilität der Cisco Software und Hardware jeder unterstützten Version, einschließlich Anforderungen an Betriebssystem und Hosting-Umgebung, enthalten.

Die folgende Abbildung zeigt die Secure Firewall 6100-Serie.

Abbildung 1: CSF-6160 und CSF-6170



In der folgenden Tabelle sind die Merkmale und Funktionen der Secure Firewall 6100-Serie aufgelistet.

Tabelle 1: CSF-6160 und CSF-6170 – Merkmale

Merkmale	CSF-6160	CSF-6170
Formfaktor	2 HE Für branchenübliche 19-Zoll-Racks (48,3 cm)	
Rackmontage	Zwei Gleitschienen-Montagehalterungen und zwei Gleitschienen EIA-310-D-Rack (Electronic Industries Association) mit 4 Säulen	
Luftstromführung	Von vorne nach hinten (E/A-Seite zu Nicht-E/A-Seite) Kaltgang zu Warmgang	
Systemspeicher	24 x 64 GB	24 x 96 GB
Management-Ports	Zwei 1/10/25-Gbit/s-SFP28-Ports	
Konsolen-Port	Eine Cisco Seriennummer (RS-232 auf RJ-45)	
USB-Port	Ein USB 3.0-Port vom Typ A, 5 W	
Netzwerk-Anschlüsse	Zwölf fest konfigurierte SFP56-Glasfaser-Ports mit 1/10/25/50 Gbit/s (Bezeichnung Ethernet 1/1 bis 1/12) Vier fest konfigurierte QSFP56-Ports mit 4x40/100/200 Gbit/s (Bezeichnung Ethernet 1/13 bis 1/16)	
Netzwerkmodule	Zwei (Hot-Swap-fähig) Hinweis Hot-Swapping identischer Module wird unterstützt. Wenn Sie allerdings ein Netzwerkmodul durch einen anderen Typ ersetzen, müssen Sie das System neu starten, damit das neue Netzwerkmodul erkannt wird.	

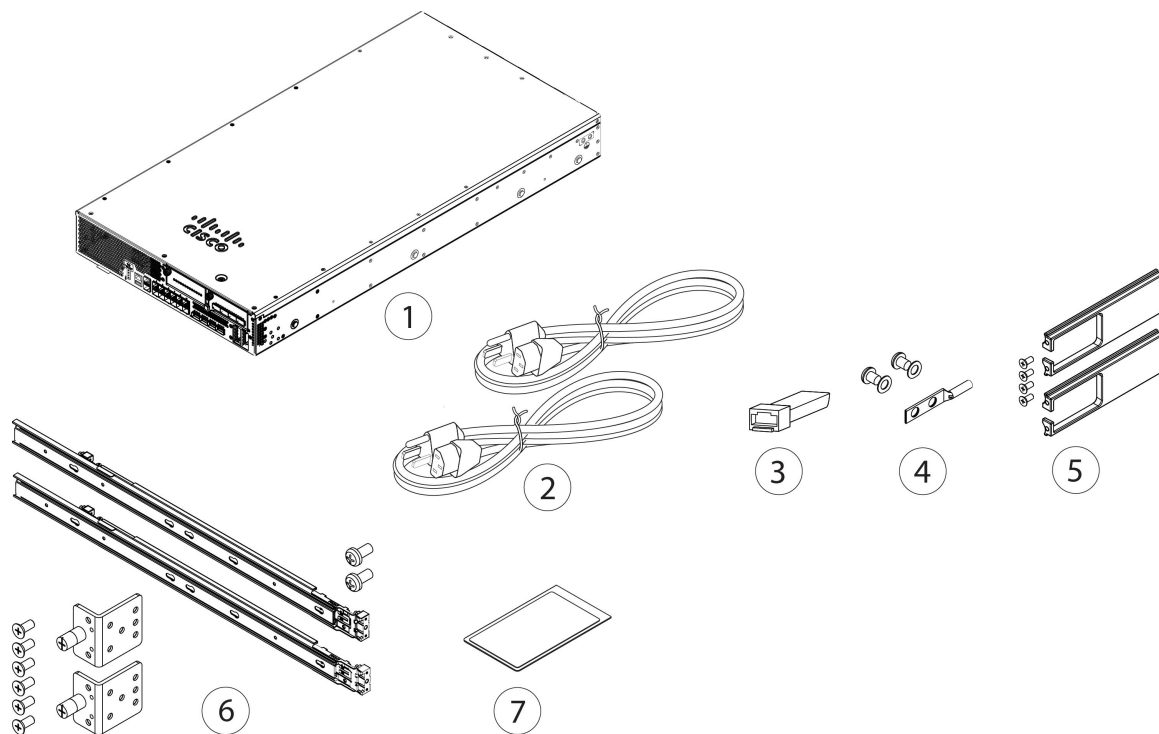
Merkmal	CSF-6160	CSF-6170
Unterstützte Netzwerkmodule	<ul style="list-style-type: none"> • 1/10-Gbit/s-SFP+ mit 8 Ports (CSF6K-XNM-8X10G) • 1/10/25-Gbit/s-SFP+ mit 8 Ports (CSF6K-XNM-8X25G) • 4-Gbit/s-QSFP/QSFP+ mit 4 Ports (CSF6K-XNM-4X40G) • 40/100/200-Gbit/s-QSFP56/QSFP mit 4 Ports (CSF6K-XNM-4X200G) • 100-Gbit/s-QSFP56/QSFP28/QSFP mit 2 Ports (CSF6K-XNM-2X100G) • 1-Gbit/s-SFP-SX-Multimode-Hardwareumgebung mit 6 Ports (CSF6K-XNM-6X1SXF) • 10-Gbit/s-SFP-SR-Multimode-Hardwareumgebung mit 6 Ports (CSF6K-XNM-6X10SRF) • 10-Gbit/s-SFP-LR-Singlemode-Hardwareumgebung mit 6 Ports (CSF6K-XNM-6X10LRF) • 25-Gbit/s-SFP-SR-Multimode-Hardwareumgebung mit 6 Ports (CSF6K-XNM-6X25SRF) • 25-Gbit/s-SFP-LR-Singlemode-Hardwareumgebung mit 6 Ports (CSF6K-XNM-6X25LRF) • 1-Gbit/s-Kupfer-1000Base-T-Hardwareumgebung mit 8 Ports (CSF6K-XNM-8X1GF) • 400-Gbit/s-QSFP-DD mit 2 Ports (CSF6K-XNM-2X400G) 	
Netzteil	<p>Zwei AC/DC-Hochspannungsnetzteile</p> <p>Unterstützt HVAC, HVDC und LVDC (-48 VDC)</p> <ul style="list-style-type: none"> • AC-Hochbereichsspannung: Bis zu 3.000 W pro Netzteil, Redundanz mit Lastverteilung, im laufenden Betrieb austauschbar • AC-Niedrigbereichsspannung: Bis zu 1.500 W pro Netzteil, Lastverteilung ohne Redundanz • Beide Gleichstrom-Eingänge verbunden: Bis zu 3.000 W pro Netzteil, Redundanz mit Lastverteilung, im laufenden Betrieb austauschbar • Ein Gleichstromeingang verbunden: Bis zu 1.500 W pro Netzteil, Lastverteilung ohne Redundanz 	
Redundante Spannungsversorgung	<p>Ja</p> <p>1 + 1-Redundanz mit zwei HVAC/HVDC-Modulen oder zwei LVDC-Eingängen</p> <p>Hinweis Zwei Netzteile sind im Lieferumfang enthalten.</p>	

Merkmal	CSF-6160	CSF-6170
Lüfter	Vier redundante Lüftermodule mit zwei Lüftern; jedes Modul hat 2 Lüfter (Hot-Swap-fähig)	
Speicher	Zwei SSD-Laufwerke Zwei 3,6-TB-SSDs im Lieferumfang enthalten; werkseitig für RAID1 konfiguriert.	Zwei SSD-Laufwerke Zwei 7,2-TB-SSDs im Lieferumfang enthalten; werkseitig für RAID1 konfiguriert.
Herausnehmbare Anlagenkarte	Zeigt die Seriennummer und einen QR-Code an, der auf das Dokumentationsportal verweist.	
Erdung	Erdungs-Pad an der linken Seite des Chassis (von der Rückseite aus gesehen)	
Power-Taste:	Steuert die Stromversorgung des Systems; an der Vorderseite links Weitere Informationen zur Power-Taste finden Sie unter Power-Taste und Reset-Taste, auf Seite 9 .	
Reset-Taste	Setzt das System auf die Werkseinstellungen zurück, ohne dass dafür auf die serielle Konsole zugegriffen werden muss; an der Vorderseite links. Weitere Informationen zur Reset-Taste finden Sie unter Power-Taste und Reset-Taste, auf Seite 9 .	

Lieferumfang

Die folgende Abbildung zeigt den Lieferumfang für die Secure Firewall 6100. Dieser kann jedoch variieren, und Ihre Lieferung kann mehr oder weniger Artikel umfassen, falls Sie zusätzliche Teile bestellt haben. Unter [Produkt-IDs, auf Seite 50](#) finden Sie eine Liste der dem Lieferumfang zugehörigen PIDs.

Abbildung 2: CSF-6160 und CSF-6170 – Lieferumfang



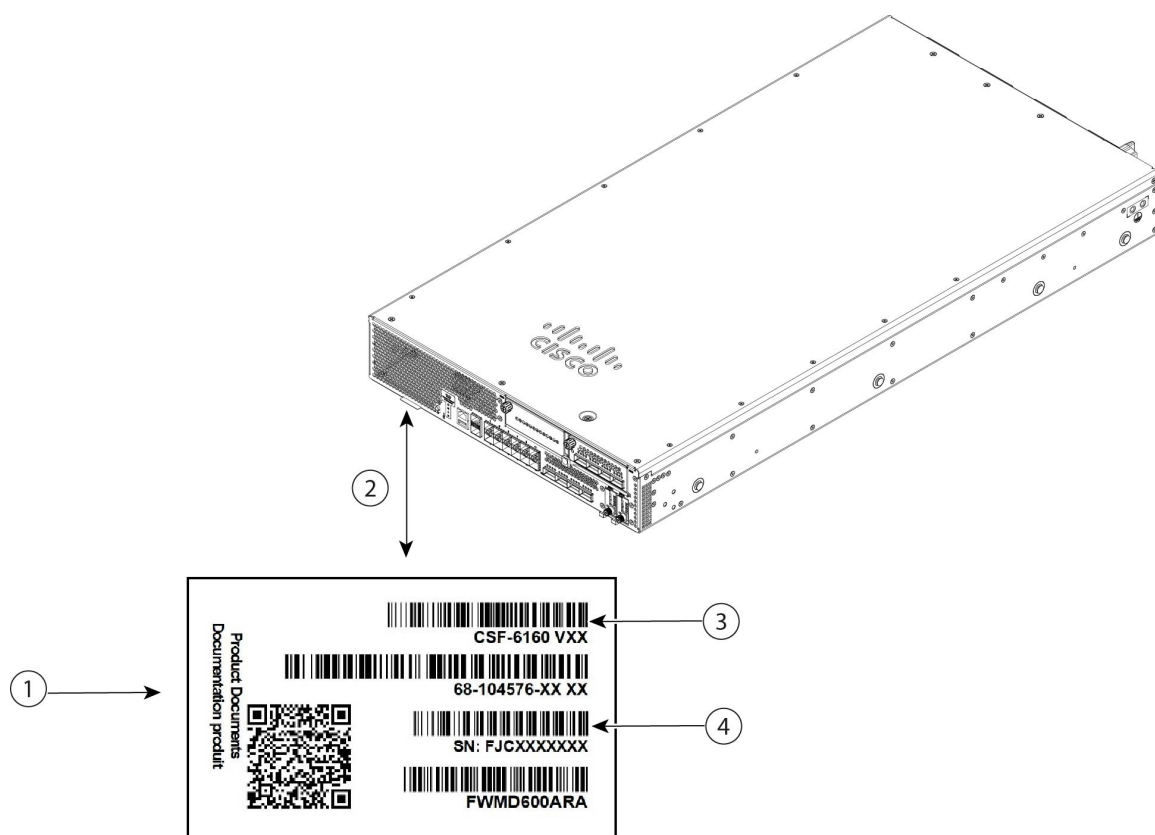
1	Secure Firewall 6100-Serie	2	Zwei Netzkabel (länderspezifisch) Eine Liste der unterstützten Netzkabel finden Sie unter Netzkabelspezifikationen , auf Seite 53.
3	SFP-Transceiver (Optional; im Lieferumfang enthalten, sofern bestellt)	4	Erdungslasche, Schrauben und Unterlegscheiben <ul style="list-style-type: none"> • Eine Erdungslasche mit 6AWG 0,25-Zoll-Lochdurchmesser • Zwei 1/4-20 x 0,297-Zoll-Schrauben • Zwei T-Unterlegscheiben mit 0,469 Zoll AD, 0,261 Zoll ID und 0,025 Zoll
5	Kabelmanagement-Halteklammer-Kit <ul style="list-style-type: none"> • Zwei Kabelmanagement-Halteklammern • Vier Kreuzschlitzschrauben (8–32 x 0,375-Zoll) (Optional; im Lieferumfang enthalten, sofern bestellt)	6	Gleitschienen-Zubehör-Kit: <ul style="list-style-type: none"> • Zwei Gleitschienen • Zwei Gleitschienen-Montagehalterungen • Sechs Kreuzschlitzschrauben (8–32 x 0,302-Zoll) für die Gleitschienen-Montageklammern zur Befestigung der Halterungen am Chassis • Zwei Kreuzschlitzschrauben (M3 x 0,5 x 6 mm) zur Befestigung des Chassis an Ihrem Rack

<p>7 <i>Cisco Secure Firewall 6100</i></p> <p>Dieses Dokument enthält Links zum Hardware-Installationshandbuch, zum Handbuch zu gesetzlichen Auflagen und Sicherheits-hinweisen sowie zu Garantie- und Lizenzierungsinformationen. Es enthält außerdem einen QR-Code und eine URL, die auf das Portal für digitale Dokumentation verweisen. Das Portal enthält Links zur Seite mit Produktinformationen, zum Hardware-Installationshandbuch, zum Handbuch zu gesetzlichen Vorschriften und Sicherheitshinweisen und zum Leitfaden zu den ersten Schritten.</p>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Seriennummer und QR-Code für das Dokumentationsportal

Die herausziehbare Anlagenkarte an der Vorderseite des Secure Firewall 6100-Chassis enthält die Chassis-Seriennummer und den QR-Code für das Dokumentationsportal, der auf den Leitfaden zu den ersten Schritten, den Leitfaden zu rechtlichen Anforderungen und Compliance und das Hardware-Installationshandbuch verweist.

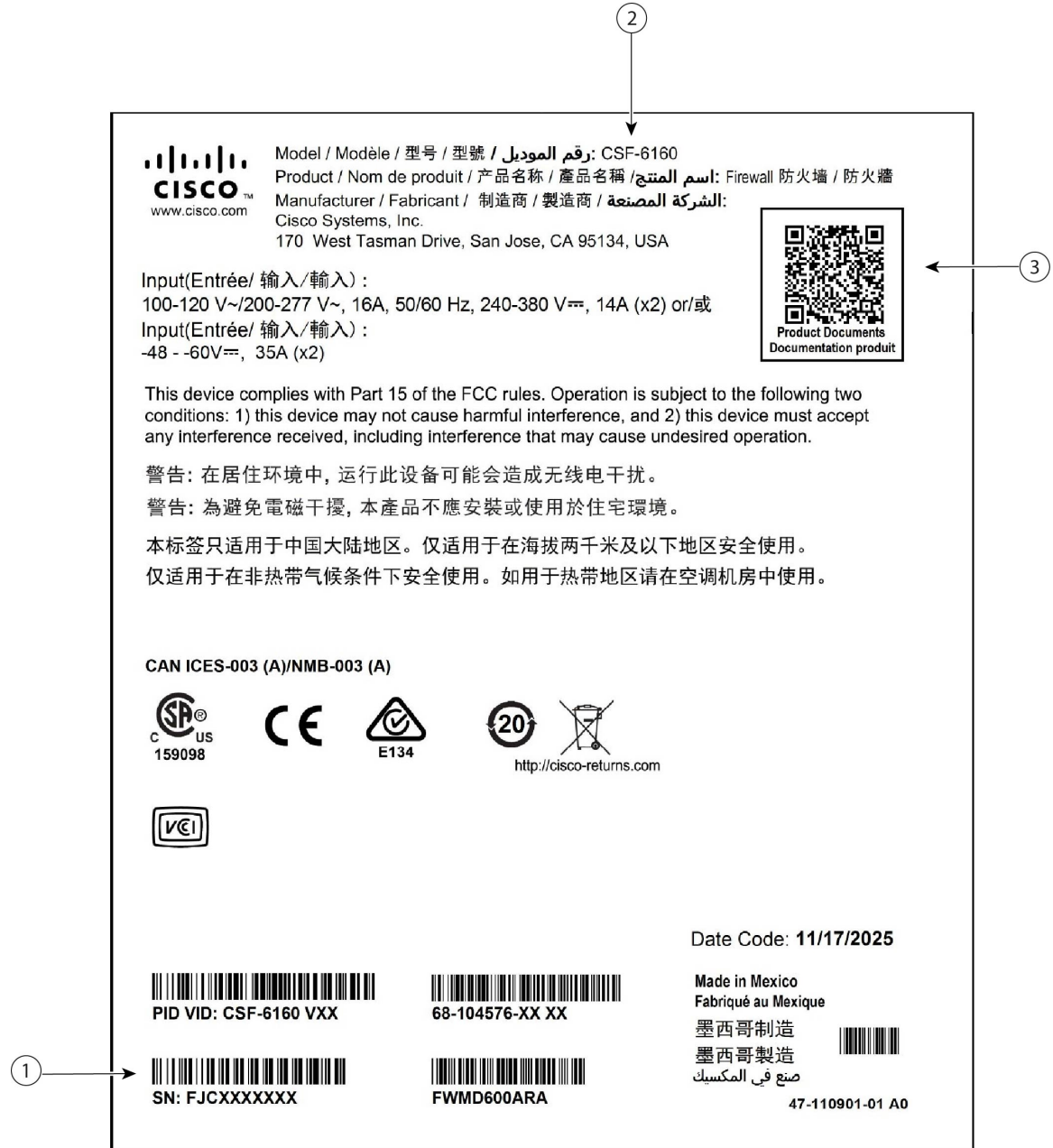
Abbildung 3: Herausnehmbare Anlagenkarte



1	Herausziehbares Anlagen-Tag	2	QR-Code des Portals für Dokumentation
3	Chassis-Modellnummer	4	Chassis-Seriennummer

Die Compliance-Kennzeichnung an der Unterseite des Chassis enthält die Chassis-Seriennummer, Kennzeichnungen zur gesetzlichen Compliance sowie den QR-Code des Portals für Dokumentation, der auf die oben angegebenen Leitfäden verweist. Die folgende Abbildung zeigt ein Beispiel eines Konformitätsschilds, das sich auf der Unterseite des Gehäuses befindet.

Abbildung 4: Konformitätsschild (Beispiel)

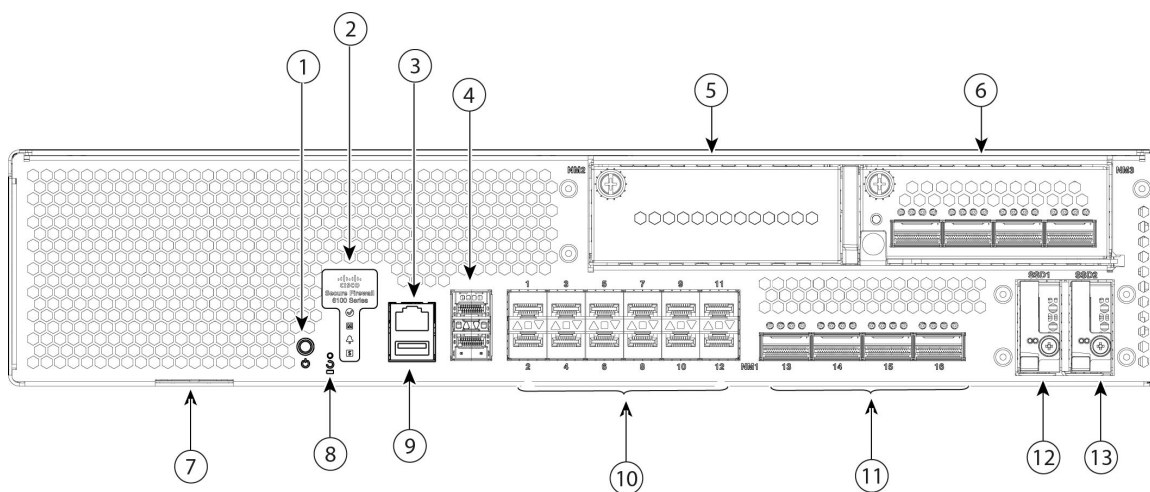


1	Seriennummer	2	Chassis-Modellnummer
3	QR-Code des Portals für Dokumentation		—

Vorderseite

Die folgende Abbildung zeigt die Vorderseite der Secure Firewall 6100-Serie. Unter [LEDs an der Vorderseite](#), auf Seite 12 finden Sie eine Beschreibung der LEDs.

Abbildung 5: CSF-6160 und CSF-6170 – Vorderseite



1	EIN/AUS-Taste Multifunktions-Drucktaste, die den Vorgang zum Aus- und Wiedereinschalten, Herunterfahren und Einschalten steuert.	2	System-LEDs
3	RJ-45 (8P8C) Konsolen-Port	4	Dual-Stack-Management-Ports (unterstützen 1/10/25 Gbit/s) Oberer Port: <ul style="list-style-type: none"> • Cisco Secure Firewall Threat Defense – Management 0 (auch als Management 1/1 bezeichnet) • ASA – Management 1/1 Unterer Port: <ul style="list-style-type: none"> • Cisco Secure Firewall Threat Defense – Management 1 (auch als Management 1/2 bezeichnet) • ASA – Management 1/2

5	Steckplatz für Netzwerkmodul (NM-2)	6	Steckplatz für Netzwerkmodul (NM-3)
7	Herausziehbare Anlagenkarte mit Chassis-Seriennummer und QR-Code zum Portal für die digitale Dokumentation. Dort finden Sie Links zum Leitfaden zu den ersten Schritten, zum Hardwareleitfaden sowie zum Leitfaden zu gesetzlichen Auflagen und Compliance.	8	Versenkte Taste zum Zurücksetzen auf die Werkseinstellungen
9	USB 3.0-Port, Typ A	10	Zwölf fest konfigurierte SFP56-Glasfaser-Ports mit 1/10/25/50 Gbit/s (NM-1) Glasfaser-Ports mit den Bezeichnungen 1/1 bis 1/12 (von links nach rechts)
11	Vier fest konfigurierte QSFP56-Glasfaser-Ports mit 40/100/200 Gbit/s (NM-1) Glasfaser-Ports mit den Bezeichnungen 1/13 bis 1/16 (von links nach rechts)	12	SSD-Steckplatz (SSD-1)
13	SSD-Steckplatz (SSD-2)		—

Power-Taste und Reset-Taste

Die Secure Firewall 6100-Serie verfügt über eine Power-Taste an der Vorderseite, die die Stromversorgung des Systems steuert. Das System wird automatisch eingeschaltet, wenn Wechselstrom angeschlossen wird. Die Taste ist EIN, wenn sie hineingedrückt wird, und AUS, wenn sie herausragt. Wenn Sie das System Aus- und Wiedereinschalten möchten, halten Sie die Taste 5 Sekunden lang gedrückt. Um ein ordnungsgemäßes Herunterfahren einzuleiten, halten Sie sie 15 Sekunden lang gedrückt. Warten Sie immer, bis die LEDs erloschen sind, bevor Sie die Netzkabel abziehen, um Laufwerksbeschädigungen zu vermeiden.

Eine versenkte Taste zum Zurücksetzen auf die Werkseinstellungen ist ebenfalls vorhanden. Durch 5 Sekunden langes Eindrücken der Taste wird das System auf die Werkseinstellungen zurückgesetzt. Konfigurationen und Benutzerdateien werden dabei gelöscht. Verwenden Sie diese Funktion, wenn Anmeldeinformationen verloren gegangen sind und kein Zugriff auf die Konsole möglich ist. Wenn die Stromversorgung während des Zurücksetzungsvorgangs ausfällt, muss der Prozess nach Wiederherstellung der Stromversorgung neu gestartet werden.

Power-Taste:

Die Power-Taste ist ein nicht verriegelnder Druckschalter zur Steuerung der Stromversorgung des Systems. Sie befindet sich auf der Vorderseite links. Wenn die Wechselstromversorgung zum ersten Mal eingeschaltet wird, müssen Sie die Taste nicht drücken, da das System standardmäßig eingeschaltet wird. Während des Herunterfahrens blinken die Betriebsanzeige-LEDs grün, um anzuzeigen, dass der Prozess gestartet wurde. Nach dem Herunterfahren wird das System ausgeschaltet. Warten Sie, bis die Betriebsanzeige-LEDs durchgehend orange leuchten, bevor Sie die Wechselstromkabel abziehen. Unter [LEDs an der Vorderseite](#), auf Seite 12 finden Sie eine detaillierte Beschreibung der Betriebsanzeige-LED.

Bei der ROMMON- oder FX-OS-Eingabeaufforderung:

- Halten Sie die Power-Taste 5 Sekunden lang gedrückt und lassen Sie sie los, um ein Aus- und Wiedereinschalten des Systems einzuleiten. Die Betriebsanzeige-LED blinkt grün mit einer Frequenz von 2 Hz.
- Halten Sie die Power-Taste 15 Sekunden lang gedrückt und lassen Sie sie los, um ein ordnungsgemäßes Herunterfahren einzuleiten. Die Betriebsanzeige-LED blinkt grün mit einer Frequenz von 10 Hz.



Hinweis Threat Defense erfordert ein ordnungsgemäßes Herunterfahren. Einzelheiten zur zugehörigen Vorgehensweise finden Sie im Leitfaden für die ersten Schritte.



Hinweis Nachdem Sie das Chassis von der Stromversorgung getrennt haben, warten Sie mindestens 10 Sekunden, bevor Sie die Stromversorgung wieder einschalten. Lassen Sie das System, einschließlich der Standby-Stromversorgung, 10 Sekunden lang ausgeschaltet.



Vorsicht Wenn Sie die Netzkabel des Systems abziehen, bevor das ordnungsgemäße Herunterfahren abgeschlossen ist, kann die Festplatte beschädigt werden.

Taste zum Zurücksetzen auf die Werkseinstellungen

Das Secure Firewall 6100-Serie-Chassis verfügt über eine versenkte Reset-Taste zum Zurücksetzen des Systems auf die Werkseinstellungen. Wenn die Taste fünf Sekunden lang gedrückt wird, werden die aktuelle Konfiguration und die aktuellen Dateien gelöscht.



Hinweis Verwenden Sie die Reset-Taste, wenn die aktuellen Anmeldeinformationen verloren gegangen sind und Sie das System ohne Konsolenzugriff initialisieren möchten.

Folgendes geschieht:

- Der ROMMON-NVRAM wird gelöscht und auf die Standardeinstellungen zurückgesetzt.
- Alle zusätzlichen Images werden entfernt. Das aktuell ausgeführte Image bleibt bestehen.
- FXOS-Protokolle, Core-Dateien, SSH-Schlüssel, Zertifikate, FXOS-Konfiguration und Apache-Konfiguration werden entfernt.



Hinweis Wenn die Stromversorgung zwischen dem Drücken der Reset-Taste und dem Abschluss des Zurücksetzvorgangs unterbrochen wird, stoppt der Prozess, und Sie müssen die Taste erneut drücken, sobald das System wieder mit Strom versorgt wird.

Management-Port, Konsolen-Port und USB-Port

Management-Port

Das Chassis der Secure Firewall 6100 verfügt über zwei Management-Ports. Es handelt sich um SFP28-Ports mit 1/10/25-Gbit/s, die sowohl Glasfaser als auch DAC- oder GLC-TE unterstützen.

RJ-45-Konsolen-Port

Die Secure Firewall 6100-Serie wird nicht mit einem seriellen RJ-45-Kabel ausgeliefert, es sei denn, Sie bestellen es zusammen mit dem Chassis. Passende Kabel, z. B. ein serielles USB-zu-RJ-45-Kabel, sind separat erhältlich. Sie können mithilfe der CLI Ihre Secure Firewall 6100-Serie über den seriellen RJ-45-Konsolen-Port konfigurieren. Verwenden Sie dazu einen Terminal-Server oder ein Terminal-Emulationsprogramm über einen Computer.

Der RJ-45-Port (8P8C) unterstützt die RS-232-Signalübertragung an einen internen UART-Controller. Der Konsolen-Port hat keine Hardware-Flusskontrolle und unterstützt keine Remote-Einwahlmodems. Die Standard-Konsolen-Port-Einstellungen werden wie folgt angezeigt:

- 9.600 BAUD-Rate
- 8 Daten-Bits
- Keine Parität
- 1 Stopp-Bit
- Keine Flusskontrolle

USB 3.0-Port, Typ A

Sie können am externen USB-A-Port ein Datenspeichergerät anschließen. Die Kennung für das externe USB-Laufwerk lautet `usb:`. Der USB-A-Port unterstützt Folgendes:

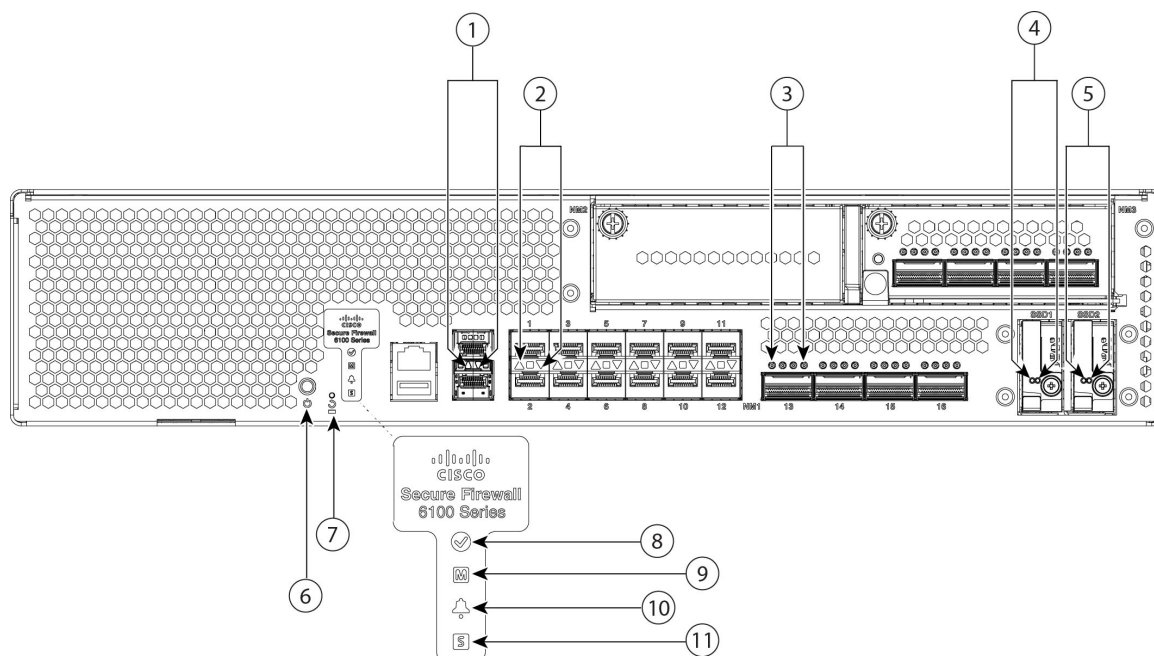
- Austausch im laufenden Betrieb
- Mit FAT32 formatiertes USB-Laufwerk
- Boot-KickstartImage von ROMMON zu Recovery-Zwecken
- Kopieren Sie diese nach und von `workspace:/` und `volatile:/` im `local-mgmt`-Befehlsmodus. Die relevantesten Dateien sind:
 - Hauptdateien
 - EthAnalyzer-Paketerfassungen
 - Dateien für den technischen Support
 - Sicherheitsmodul-Protokolldateien
- Upload des Plattform-Bundle-Images mithilfe von **download image usbA:**

Der USB-Port vom Typ A bietet *keine* Unterstützung für den Cisco Secure Package-Image-Upload (CSP-Image-Upload).

LEDs an der Vorderseite

Die folgende Abbildung zeigt die LEDs an der Vorderseite der Cisco Secure Firewall 6100-Serie.

Abbildung 6: CSF-6160 und CSF-6170 – LEDs an der Vorderseite



<p>1 Management-Port</p> <p>Der 1/10/25-Gbit/s-Glasfaser-Management-Port verfügt über eine zweifarbige LED unter dem SFP-Gehäuse, die Verbindung/Aktivität/Fehler anzeigt:</p> <ul style="list-style-type: none"> • Aus: Kein SFP. • Grün: Verbindung aktiv. • Grün blinkend: Netzwerkaktivität. • Orange: SFP vorhanden, aber kein Link. 	<p>2 Verbindungs-/Aktivitätsstatus der fest konfigurierten Glasfaser-Ports</p> <p>Jeder Glasfaser-Port verfügt über eine zweifarbige LED unter dem SFP-Gehäuse.</p> <ul style="list-style-type: none"> • Aus: Kein SFP. • Grün: Verbindung ist betriebsbereit und aktiv. • Grün blinkend: Netzwerkaktivität. • Orange: Keine Verbindung oder Netzwerkausfall.
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

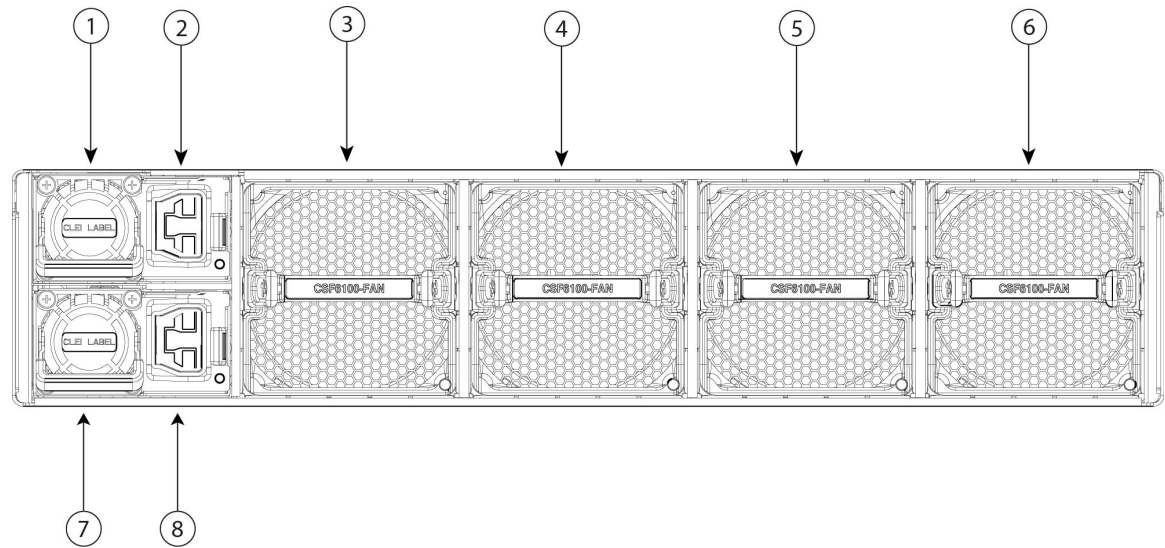
<p>3 Verbindung/Aktivität an fest konfiguriertem QSFP-Port</p> <p>Jeder Glasfaser-Port verfügt über eine zweifarbige LED unter dem QSFP-Gehäuse.</p> <ul style="list-style-type: none"> • Aus: Kein SFP. • Grün: Verbindung ist betriebsbereit und aktiv. • Grün blinkend: Netzwerkaktivität. • Orange: Keine Verbindung oder Netzwerkausfall. <p>Hinweis Die einzelnen QSFP-Steckplätze verfügen jeweils über vier LEDs.</p> <p>Bei nativem 40/100/200 Gbit/s ist nur die linke LED aktiv (von 4 LEDs pro Port). Im 4x10/25G/50G-Breakout-Modus sind jedoch alle vier LEDs an einem Port aktiv und verhalten sich entsprechend der Aktivität des jeweiligen Kanals.</p>	<p>4 SSD-1</p> <p>Hinweis Die linke LED ist aktiv. Die rechte LED ist immer aus.</p> <ul style="list-style-type: none"> • Aus: Es ist keine SSD vorhanden. • Grün: Die SSD ist vorhanden, aber nicht aktiv. • Grün blinkend: Die SSD ist aktiv. • Orange: Bei der SSD liegt ein Problem oder ein Fehler vor.
<p>5 SSD-2</p> <p>Hinweis Die linke LED ist aktiv. Die rechte LED ist immer aus.</p> <ul style="list-style-type: none"> • Aus: Es ist keine SSD vorhanden. • Grün: Die SSD ist vorhanden, aber nicht aktiv. • Grün blinkend: Die SSD ist aktiv. • Orange: Bei der SSD liegt ein Problem oder ein Fehler vor. 	<p>6 Strom</p> <ul style="list-style-type: none"> • Aus: Das System ist ausgeschaltet. Wenn das AC-Netzkabel eingesteckt ist und die LED am Netzteil grün blinkt, ist die Standby-Stromversorgung weiterhin aktiv. • Grün blinkend: Das System hat erkannt, dass die Power-Taste betätigt wurde, und hat mit dem Herunterfahren begonnen. Entfernen Sie nicht die AC- oder DC-Stromquelle, während diese LED blinkt, damit das System Zeit hat, ordnungsgemäß herunterzufahren. • Grün: Das System wurde vollständig gebootet. • Orange: Ein ordnungsgemäßes Herunterfahren wurde abgeschlossen oder es wurden Stromausfälle im System erkannt.

<p>7 Taste zum Zurücksetzen auf die Werkseinstellungen</p> <ul style="list-style-type: none"> • Grün blinkend: Blinkt 5 Sekunden nach dem Drücken der Taste. • Aus: Das Zurücksetzen ist abgeschlossen. <p>Hinweis Die Taste zum Zurücksetzen auf die Werkseinstellungen beginnt zu blinken, nachdem sie mindestens 5 Sekunden lang gedrückt wurde. Die Taste leuchtet dann, bis die Software alle Werkseinstellungen vollständig übernommen hat oder der Vorgang durch Aus- und Wiedereinschalten unterbrochen wird.</p>	<p>8 Aktiv (Rolle des Hochverfügbarkeitspaars)</p> <ul style="list-style-type: none"> • Aus: Die Einheit ist nicht konfiguriert oder in einem Hochverfügbarkeitspaar aktiviert. • Grün: Die Einheit befindet sich im aktiven Modus. • Gelb: Die Einheit befindet sich im Standby-Modus.
<p>9 Managed</p> <p>Reserviert für künftige Verwendung.</p>	<p>10 Alarm</p> <ul style="list-style-type: none"> • Aus: Während das System eingeschaltet und hochgefahren wird. • Gelb: Ausfall des Netzteils, Temperatur zu hoch und/oder Lüfterausfall. • Grün: Keine Alarme.
<p>11 System</p> <ul style="list-style-type: none"> • Aus: Während das System hochfährt. • Grün, schnell blinkend: Bootvorgang wird ausgeführt. • Grün: Normale Systemfunktion. • Gelb: Der Bootvorgang des Systems ist fehlgeschlagen. • Gelb blinkend: Alarmzustand, das System muss gewartet werden oder es ist ein Benutzereingriff erforderlich, und es bootet möglicherweise nicht ordnungsgemäß. 	<p>—</p>

Rückseite

Die folgende Abbildung zeigt die Rückseite der Secure Firewall 6100-Serie. Eine Beschreibung der LEDs des Netzteil- und Lüftermoduls finden Sie unter [Netzstrommodule, auf Seite 29](#) und [Lüftermodule, auf Seite 31](#).

Abbildung 7: Rückseite von CSF-6160 und CSF-6170



1	Netzteilmodul (PSU-1)	2	Steckverbinder für Netzteilmodul 1 (PSU-1)
3	Duales Lüftermodul 1 (FAN-1)	4	Duales Lüftermodul 2 (FAN-2)
5	Duales Lüftermodul 3 (FAN-3)	6	Duales Lüftermodul 4 (FAN-4)
7	Netzteilmodul (PSU-2)	8	Steckverbinder für Netzteilmodul (PSU-2)

Weitere Informationen

- Unter [Entfernen und Austauschen des Netzteilmoduls, auf Seite 94](#) finden Sie die Vorgehensweise für den Ausbau und Austausch des Netzteilmoduls bei der Secure Firewall 6100-Serie.
- Unter [Lüftermodule, auf Seite 31](#) finden Sie die Vorgehensweise für den Ausbau und Austausch des dualen Lüftermoduls bei der Secure Firewall 6100-Serie.
- Unter [Erdung des Chassis, auf Seite 85](#) finden Sie die Vorgehensweise zur Erdung des Chassis mithilfe der Erdungsklemme.
- Unter [Netzstrommodule, auf Seite 29](#) finden Sie eine Beschreibung der LEDs des Netzteilmoduls.
- Unter [Lüftermodule, auf Seite 31](#) finden Sie eine Beschreibung der LEDs des Lüfters.

1/10/25-Gbit/s-Netzwerkmodul mit 8 Ports (CSF6K-XNM-8X10G)

Unter [Unterstützte Transceiver, auf Seite 33](#) finden Sie Informationen zur Softwareversion und Transceiver-Unterstützung für dieses Netzwerkmodul.

Das Chassis der Secure Firewall 6100 verfügt über zwei Netzwerkmodul-Steckplätze mit den Bezeichnungen NM-2 und NM-3 (von links nach rechts an der Vorderseite). Netzwerkmodule sind optionale, herausnehmbare I/O-Module, die entweder zusätzliche Ports oder verschiedene Schnittstellentypen bereitstellen. Das Netzwerkmodul wird auf der Vorderseite des Chassis angeschlossen. Unter [Vorderseite, auf Seite 8](#) finden Sie Informationen zur Position der Netzwerkmodul-Steckplätze am Chassis.

CSF6K-XNM-8X10G unterstützt Vollduplex-Ethernet-Traffic mit 1 Gbit/s- und 10 Gbit/s pro Port und wird von allen Secure Firewall 6100-Modellen unterstützt. FPR6K-XNM-8X25G unterstützt Vollduplex-Ethernet-Traffic mit 1 Gbit/s, 10 Gbit/s oder 25 Gbit/s pro Port und wird von allen Secure Firewall 6100-Modellen unterstützt.

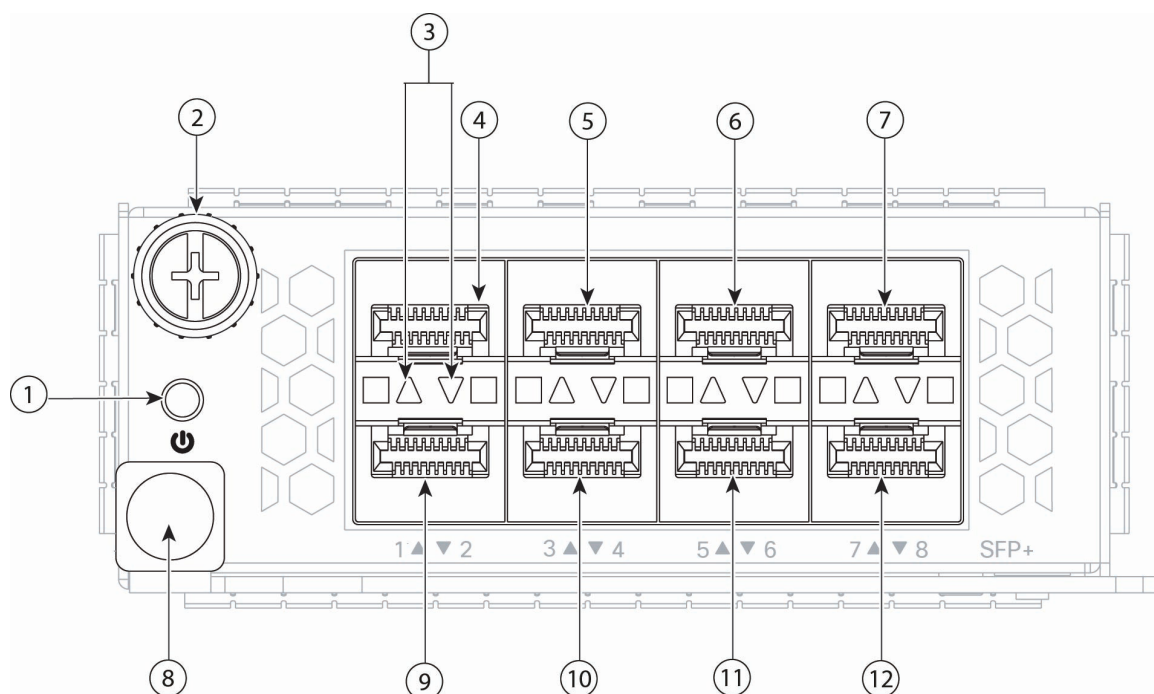
Die oberen Ports sind von links nach rechts nummeriert: Ethernet 2/1 oder 3/1, Ethernet 2/3 oder 3/3, Ethernet 2/5 oder 3/5 und Ethernet 2/7 oder 3/7. Die unteren Ports sind von links nach rechts nummeriert: Ethernet 2/2 oder 3/2, Ethernet 2/4 oder 3/4, Ethernet 2/6 oder 3/6 und Ethernet 2/8 oder 3/8 (siehe Abbildung unten). Die nach oben zeigenden Pfeile verweisen auf die oberen Ports, die nach unten zeigenden Pfeile auf die unteren Ports (siehe Abbildung unten). Dieses Netzwerkmodul unterstützt SFP-/SFP+/-/SFP28-Transceiver.



Hinweis Die Hardware und das System unterstützen den Austausch im laufenden Betrieb (Hot Swap), wenn Sie ein Netzwerkmodul durch ein Netzwerkmodul desselben Typs ersetzen. Sie müssen den Netzwerk-Port zuerst deaktivieren und ihn nach dem Austausch wieder aktivieren. Wenn Sie das 1/10/25 Gbit/s-Netzwerkmodul mit 8 Ports durch ein anderes unterstütztes Netzwerkmodul ersetzen, müssen Sie das Chassis neu starten, damit das neue Netzwerkmodul erkannt wird. Weitere Informationen zum Management von Netzwerkmodulen finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

Die folgende Abbildung zeigt die Vorderseite des Netzwerkmoduls mit 1/10 Gbit/s und 1/10/25 Gbit/s.

Abbildung 8: CSF6K-XNM-8X10G mit 8 Ports und 1/10/25 Gbit/s/CSF6K-XNM-8X25G



1	Unverlierbare Schraube	2	Ethernet 2/1 oder 3/1
3	Ethernet 2/3 oder 3/3	4	Ethernet 2/5 oder 3/5
5	Ethernet 2/7 oder 3/7	6	Betriebsanzeige-LED
7	Auswurfhebel	8	Ethernet 2/2 oder 3/2

9	Ethernet 2/4 oder 3/4	10	Ethernet 2/6 oder 3/6
11	Ethernet 2/8 oder 3/8	12	<p>Netzwerkaktivitäts-LEDs</p> <p>Die nach oben zeigenden Pfeile stehen für die oberen Ports, die nach unten zeigenden Pfeile für die unteren Ports.</p> <ul style="list-style-type: none"> • Aus: Kein SFP. • Orange: Keine Verbindung oder Netzwerkausfall. • Grün: Verbindung aktiv. • Grün blinkend: Netzwerkaktivität.

40-Gbit/s-Netzwerkmodul mit 4 Ports(CSF6K-XNM-4X40G)

Unter [Unterstützte Transceiver, auf Seite 33](#) finden Sie die Softwareversion und die Transceiver-Unterstützung für dieses Netzwerkmodul.

Das Chassis der Secure Firewall 6100 verfügt über zwei Netzwerkmodul-Steckplätze mit den Bezeichnungen NM-2 und NM-3 (von links nach rechts an der Vorderseite). Netzwerkmodule sind optionale, herausnehmbare I/O-Module, die entweder zusätzliche Ports oder verschiedene Schnittstellentypen bereitstellen. Das Netzwerkmodul wird auf der Vorderseite des Chassis angeschlossen. Unter [Vorderseite, auf Seite 8](#) finden Sie Informationen zur Position der Netzwerkmodul-Steckplätze am Chassis.

CSF6K-XNM-4X40G unterstützt 40-Gbit/s-Betrieb. Dieses Netzwerkmodul bietet Vollduplex-Ethernet-Datenverkehr pro Port. Das 40 Gbit/s-Netzwerkmodul hat vier QSFP+-Ports. Die 40-Gbit/s-Ports sind von links nach rechts nummeriert: Ethernet 2/1 oder 3/1 bis Ethernet 2/4 oder 3/4.

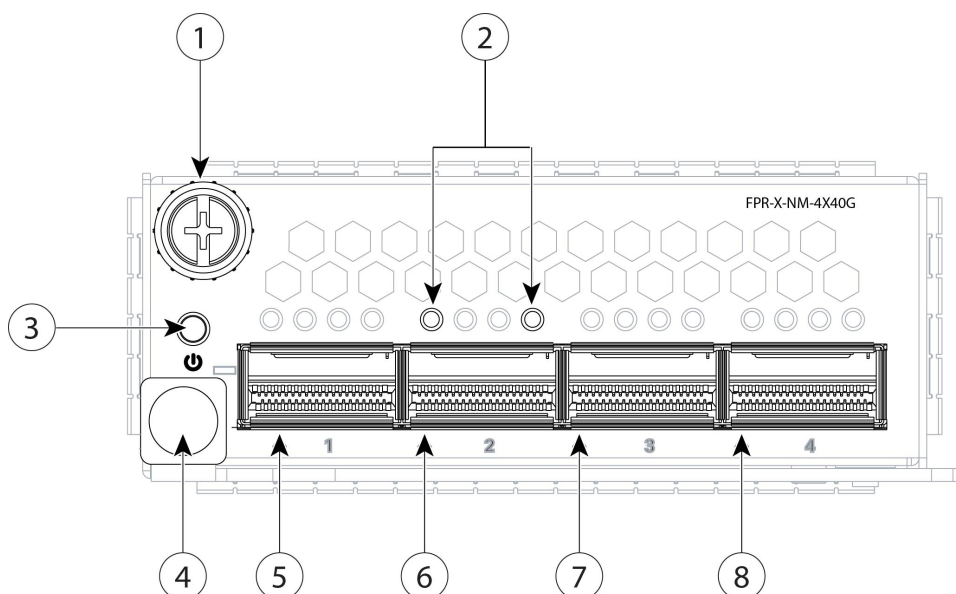
Sie können jeden der vier 40-Gbit/s-Ports mit den unterstützten Breakout-Kabeln in vier 10-Gbit/s-Ports unterteilen. Mit dem 40-Gbit/s-Netzwerkmodul mit vier Ports verfügen Sie jetzt über 16 10-Gbit/s-Schnittstellen. Die hinzugefügten Schnittstellen sind Ethernet 2/1/1 oder 3/1/1 bis Ethernet 2/4/4 oder 3/4/4.



Hinweis Die Hardware und das System unterstützen den Austausch im laufenden Betrieb (Hot Swap), wenn Sie ein Netzwerkmodul durch ein Netzwerkmodul desselben Typs ersetzen. Wenn Sie das 40 Gbit/s-Netzwerkmodul mit 4 Ports durch ein anderes unterstütztes Netzwerkmodul ersetzen, müssen Sie das Chassis neu starten, damit das neue Netzwerkmodul erkannt wird. Weitere Informationen zum Management von Netzwerkmodulen finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

Die folgende Abbildung zeigt die Vorderseite des 40-Gbit/s-Netzwerkmoduls mit 4 Ports.

Abbildung 9: CSF6K-XNM-4X40G



1	Unverlierbare Schraube	2	Netzwerkaktivitäts-LEDs Die nach oben zeigenden Pfeile stehen für die oberen Ports, die nach unten zeigenden Pfeile für die unteren Ports. <ul style="list-style-type: none">• Aus: Kein SFP.• Orange: Keine Verbindung oder Netzwerkausfall.• Grün: Die Verbindung ist aktiv.• Grün blinkend: Netzwerkaktivität.
3	Betriebsanzeige-LED	4	Auswurfhebel
5	Ethernet 2/1 oder 3/1	6	Ethernet 2/2 oder 3/2
7	Ethernet 2/3 oder 3/3	8	Ethernet 2/4 oder 3/4

2-Port-Netzwerkmodul mit 100 Gbit/s(CSF6K-XNM-2X100G)

Unter [Unterstützte Transceiver, auf Seite 33](#) finden Sie die Softwareversion und die Transceiver-Unterstützung für dieses Netzwerkmodul.

Das Chassis der Secure Firewall 6100 verfügt über zwei Netzwerkmodul-Steckplätze mit den Bezeichnungen NM-2 und NM-3 (von links nach rechts an der Vorderseite). Netzwerkmodule sind optionale, herausnehmbare I/O-Module, die entweder zusätzliche Ports oder verschiedene Schnittstellentypen bereitstellen. Das Netzwerkmodul wird auf der Vorderseite des Chassis angeschlossen. Unter [Vorderseite, auf Seite 8](#) finden Sie Informationen zur Position der Netzwerkmodul-Steckplätze am Chassis.

CSF6K-XNM-2X100G unterstützt den 40/100-Gbit/s-Betrieb. Dieses Netzwerkmodul verfügt über zwei QSFP/QSFP28-Ports und bietet Vollduplex-Ethernet-Datenverkehr pro Port. Die maximale unterstützte Bandbreite beträgt 200 Gbit/s Vollduplex, wobei jeder Port mit 100 Gbit/s betrieben wird. Die 100-Gbit/s-Ports sind von links nach rechts nummeriert: Ethernet 2/1 oder 3/1 bis Ethernet 2/2 oder 3/2.

Das Netzwerkmodul verfügt über zwei 100-Gbit/s-Ports mit der Bezeichnung E2/1 und E2/2. Sie können jeden 100-Gbit/s-Port mit den unterstützten Breakout-Kabeln in vier 10-Gbit/s- oder 25-Gbit/s-Ports aufteilen. Bei E2/1 lautet die Bezeichnung der neuen Schnittstellen E2/1/1, E2/1/2, E2/1/3 und E2/1/4. Bei E2/2 lautet die Bezeichnung der neuen Schnittstellen E2/1/2, E2/2/2, E2/2/3 und E2/2/4.



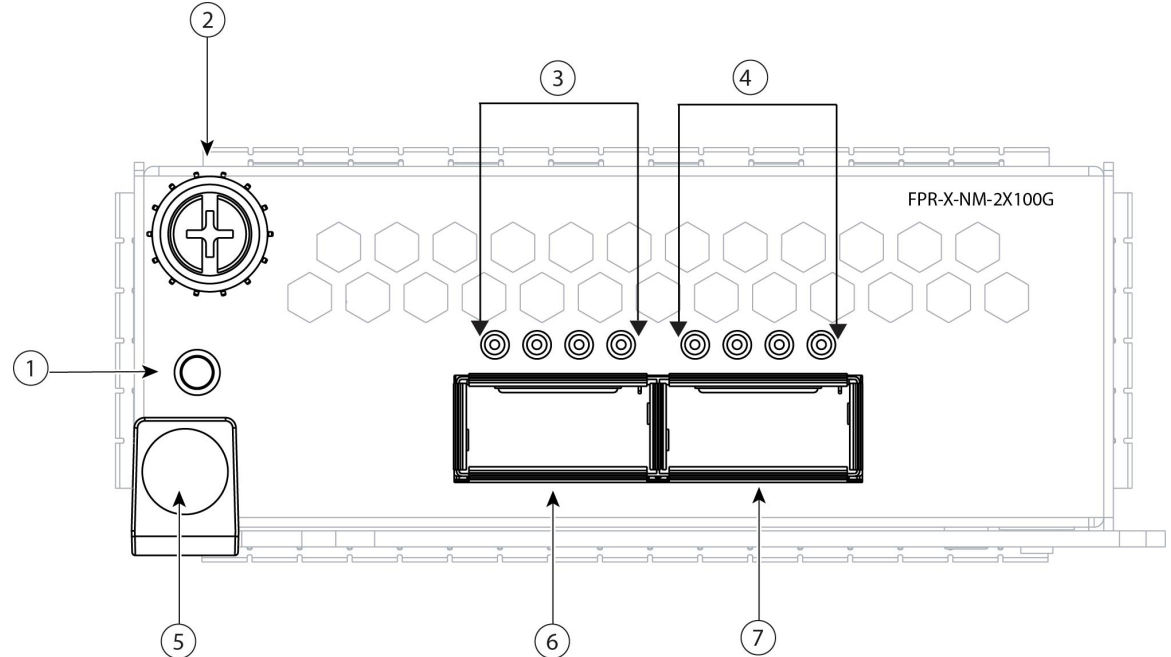
Hinweis Die Hardware und das System unterstützen den Austausch im laufenden Betrieb (Hot Swap), wenn Sie ein Netzwerkmodul durch ein Netzwerkmodul desselben Typs ersetzen. Wenn Sie das Netzwerkmodul mit 100 Gbit/s durch ein anderes unterstütztes Netzwerkmodul ersetzen, müssen Sie das Chassis neu starten, damit das neue Netzwerkmodul erkannt wird. Weitere Informationen zum Management von Netzwerkmodulen finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

Die folgende Abbildung zeigt die Vorderseite des 100-Gbit/s-Netzwerkmoduls mit 2 Ports.



Hinweis Wenn ein Port im 40-Gbit/s-Modus betrieben wird, zeigt nur die LED ganz links des Ports den Verbindungs-/Aktivitätsstatus an.

Abbildung 10: CSF6K-XNM-2X100G



1	Unverlierbare Schraube	2	Netzwerkaktivitäts-LEDs <ul style="list-style-type: none"> • Aus: Kein SFP. • Orange: Keine Verbindung oder Netzwerkausfall. • Grün: Die Verbindung ist aktiv. • Grün blinkend: Netzwerkaktivität.
3	Netzwerkaktivitäts-LEDs <ul style="list-style-type: none"> • Aus: Kein SFP. • Orange: Keine Verbindung oder Netzwerkausfall. • Grün: Die Verbindung ist aktiv. • Grün blinkend: Netzwerkaktivität. 	4	Betriebsanzeige-LED
5	Auswurfhebel	6	Ethernet 2/1 oder 3/1
7	Ethernet 2/2 oder 3/2		—

200-Gbit/s--Netzwerkmodul mit 4 Ports(CSF6K-XNM-4X200G)

Unter [Unterstützte Transceiver, auf Seite 33](#) finden Sie die Softwareversion und die Transceiver-Unterstützung für dieses Netzwerkmodul.

Das Secure Firewall -6100-Chassis verfügt über zwei Netzwerkmodul-Steckplätze mit den Bezeichnungen NM-2 und NM-3 (von links nach rechts an der Vorderseite). Netzwerkmodule sind optionale, herausnehmbare I/O-Module, die entweder zusätzliche Ports oder verschiedene Schnittstellentypen bereitstellen. Das Netzwerkmodul wird auf der Vorderseite des Chassis angeschlossen. Unter [Vorderseite, auf Seite 8](#) ist die Position der Netzwerkmodulsteckplätze am Chassis angegeben.

Das CSF6K-XNM-4X200G unterstützt den Betrieb mit 40/100/200 Gbit/s. Dieses Netzwerkmodul bietet Vollduplex-Ethernet-Datenverkehr pro Port. Das 200 Gbit/s-Netzwerkmodul verfügt über vier QSFP56-Ports. Die Ports sind von links nach rechts nummeriert: Ethernet 2/1 oder 3/1 bis Ethernet 2/4 oder 3/4.

Sie können jeden 100-Gbit/s-Port mit den unterstützten Breakout-Kabeln in vier 10-Gbit/s- oder 25-Gbit/s-Ports aufteilen. Mit dem 200-Gbit/s-Netzwerkmodul mit vier Ports verfügen Sie jetzt über 16 10-Gbit/s- oder 25-Gbit/s-Schnittstellen. Die hinzugefügten Schnittstellen sind Ethernet 2/1/1 bis Ethernet 2/1/4 Ethernet 2/1/1 oder 3/1/1 bis Ethernet 2/4/4 oder 3/4/4.



Hinweis

Die Hardware und das System unterstützen den Austausch im laufenden Betrieb (Hot Swap), wenn Sie ein Netzwerkmodul durch ein Netzwerkmodul desselben Typs ersetzen. Wenn Sie das 200-Gbit/s-Netzwerkmodul mit 4 Ports durch ein anderes unterstütztes Netzwerkmodul ersetzen, müssen Sie das Chassis neu starten, damit das neue Netzwerkmodul erkannt wird. Weitere Informationen zum Management von Netzwerkmodulen finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

400-Gbit/s-Netzwerkmodul mit 2 Ports(CSF6K-XNM-2X400G)

Unter [Unterstützte Transceiver, auf Seite 33](#) finden Sie die Softwareversion und die Transceiver-Unterstützung für dieses Netzwerkmodul.

Das Secure Firewall 6100-Chassis verfügt über zwei Netzwerkmodul-Steckplätze mit den Bezeichnungen NM-2 und NM-3 (von links nach rechts auf der Vorderseite). Netzwerkmodule sind optionale, herausnehmbare I/O-Module, die entweder zusätzliche Ports oder verschiedene Schnittstellentypen bereitstellen. Das Netzwerkmodul wird auf der Vorderseite des Chassis angeschlossen. Unter [Vorderseite, auf Seite 8](#) ist die Position der Netzwerkmodulsteckplätze am Chassis angegeben.

Das Modul CSF6K-XNM-2X400G unterstützt den 400-Gbit/s-Betrieb und ist auch auf 200 Gbit/s, 100 Gbit/s und 40 Gbit/s pro Port ausgelegt. Dieses Netzwerkmodul bietet Vollduplex-Ethernet-Datenverkehr pro Port. Das 400-Gbit/s-Netzwerkmodul unterstützt zwei QSFP-DD-Transceiver und ist auf die Unterstützung von 200-Gbit/s-QSFP56-, 100-Gbit/s-QSFP28- und 40-Gbit/s-QSFP+-Transceivern ausgelegt. Die 400-Gbit/s-Ports sind von links nach rechts nummeriert: Ethernet 2/1 oder 3/1 bis Ethernet 2/2 oder 3/2.



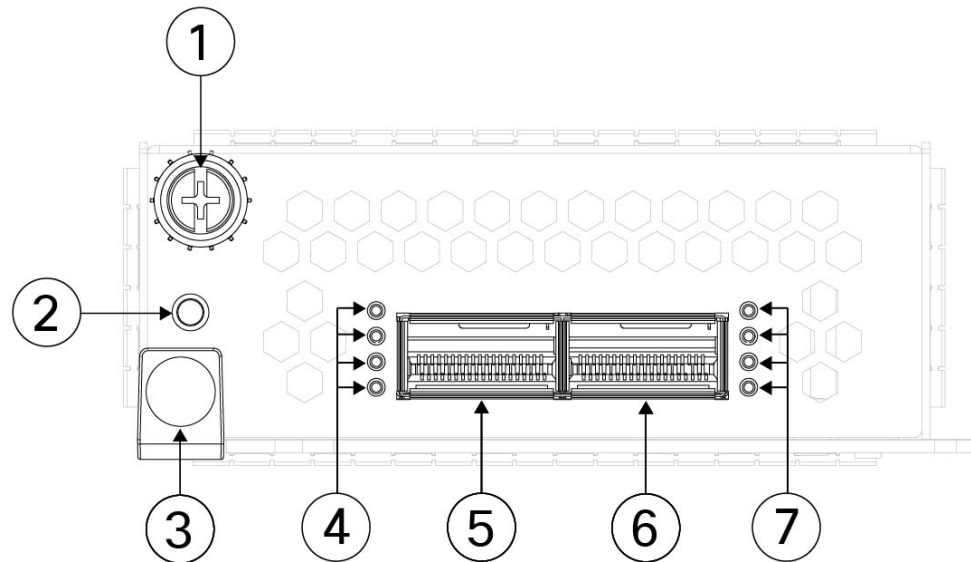
Hinweis Die Hardware und das System unterstützen den Austausch im laufenden Betrieb (Hot Swap), wenn Sie ein Netzwerkmodul durch ein Netzwerkmodul desselben Typs ersetzen. Wenn Sie das 200/400-Gbit/s-Netzwerkmodul mit 2 Ports durch ein anderes unterstütztes Netzwerkmodul ersetzen, müssen Sie das Chassis neu starten, damit das neue Netzwerkmodul erkannt wird. Weitere Informationen zum Management von Netzwerkmodulen finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

Die folgende Abbildung zeigt die Vorderseite des 200/400-Gbit/s-Netzwerkmodul mit 2 Ports.



Hinweis Wenn ein Port im 40-Gbit/s-, 100-Gbit/s- oder 200-Gbit/s-Modus betrieben wird, zeigt nur die LED ganz links den Verbindungs-/Aktivitätsstatus an.

Abbildung 12: CSF6K-XNM-2X400G



1	Unverlierbare Schraube	2	Betriebsanzeige-LED
3	Auswurfhebel	4	Netzwerkaktivitäts-LEDs <ul style="list-style-type: none"> • Aus: Kein SFP. • Orange: Keine Verbindung oder Netzwerkausfall. • Grün: Die Verbindung ist aktiv. • Grün blinkend: Netzwerkaktivität.
5	Ethernet 2/1 oder 3/1	6	Ethernet 2/2 oder 3/2
7	Netzwerkaktivitäts-LEDs <ul style="list-style-type: none"> • Aus: Kein SFP. • Orange: Keine Verbindung oder Netzwerkausfall. • Grün: Die Verbindung ist aktiv. • Grün blinkend: Netzwerkaktivität. 		—

1000Base-T-Netzwerkmodul mit Hardwareumgehung und 8 Ports (CSF6K-XNM-8X1GF)

Unter [Unterstützte Transceiver, auf Seite 33](#) finden Sie die Softwareversion und die Transceiver-Unterstützung für dieses Netzwerkmodul.

Das Chassis der Secure Firewall 6100 verfügt über zwei Netzwerkmodul-Steckplätze mit den Bezeichnungen NM-2 und NM-3 (von links nach rechts an der Vorderseite). Netzwerkmodule sind optionale, herausnehmbare I/O-Module, die entweder zusätzliche Ports oder verschiedene Schnittstellentypen bereitstellen. Das Netzwerkmodul wird auf der Vorderseite des Chassis angeschlossen. Unter [Vorderseite, auf Seite 8](#) finden Sie Informationen zur Position der Netzwerkmodul-Steckplätze am Chassis.

CSF6K-XNM-8X1GF ist ein 1000Base-T-Netzwerkmodul mit Hardwareumgehung und 8 Ports. Diese acht Ports sind von oben nach unten und von links nach rechts nummeriert. Die Ports 1 und 2, 3 und 4, 5 und 6 sowie 7 und 8 werden für den Hardwareumgehungsmodus gekoppelt. Im Hardwareumgehungsmodus werden die Daten nicht von der Secure Firewall 6100 verarbeitet, sondern an den gekoppelten Port weitergeleitet.

Eine Hardwareumgehung (auch bekannt als Fail-to-Wire) ist eine Umgehung für eine physische Schicht (Layer 1), die den Wechsel gekoppelter Schnittstellen in den Umgehungsmodus erlaubt, damit die Hardware Pakete zwischen diesen Port-Paaren ohne Softwareeingriff weiterleitet. Eine Hardwareumgehung ermöglicht Netzwerkverbindungen, wenn Software- oder Hardwarefehler auftreten. Die Hardwareumgehung ist nützlich für Ports, bei denen die Cisco Secure Firewall den Datenverkehr nur überwacht oder protokolliert. Netzwerkmodule mit Hardwareumgehung verfügen über einen Switch, der die beiden Ports bei Bedarf verbinden kann.



Hinweis Die Hardwareumgehung wird nur bei Threat Defense unterstützt, Sie können diese Module jedoch auch im Nichtumgehungsmodus in Threat Defense oder ASA verwenden.

Die Hardwareumgehung wird nur auf festgelegten Ports unterstützt. Sie können Port 1 mit Port 2 und Port 3 und Port 4 koppeln; Sie können allerdings Port 1 nicht mit Port 4 koppeln.

Wenn die Appliance vom normalen Betrieb zur Hardwareumgehung oder von der Hardwareumgehung zurück in den normalen Betrieb wechselt, kann der Datenverkehr für mehrere Sekunden unterbrochen werden. Eine Reihe von Faktoren kann sich auf die Dauer der Unterbrechung auswirken: das Verhalten des Verbindungspartners und seine Art und Weise, wie er Verbindungsfehler und die Zeitüberschreitung für das Entprellen handhabt; die Spanning Tree Protocol-Konvergenz; die Konvergenz des dynamischen Routing-Protokolls usw. Während dieser Zeit kann es zu Verbindungsunterbrechungen kommen.



Hinweis Wenn Sie einen Inline-Schnittstellensatz mit einer Kombination aus Schnittstellen mit und ohne Hardwareumgehung haben, können Sie die Hardwareumgehung für diesen Inline-Schnittstellensatz nicht aktivieren. Sie können die Hardwareumgehung für einen Inline-Schnittstellensatz nur aktivieren, wenn alle Paare im Inline-Schnittstellensatz gültige Sätze mit Hardwareumgehung sind.

Die Hardware und das System unterstützen den Austausch im laufenden Betrieb (Hot Swap), wenn Sie ein Netzwerkmodul durch ein Netzwerkmodul desselben Typs ersetzen. Wenn Sie das 1000Base-T-Netzwerkmodul mit 8 Ports durch ein anderes unterstütztes Netzwerkmodul ersetzen, müssen Sie das Chassis neu starten,

damit das neue Netzwerkmodul erkannt wird. Weitere Informationen zum Management von Netzwerkmodulen finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

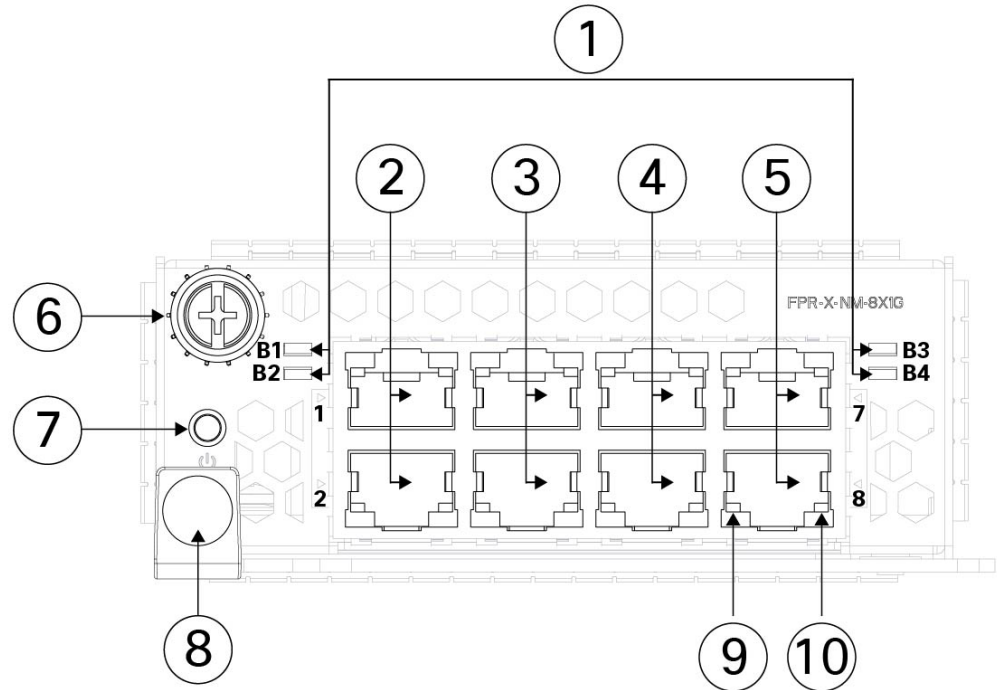
Stellen Sie sicher, dass Sie das richtige Firmwarepaket und die richtige Softwareversion installiert haben, um dieses Netzwerkmodul zu unterstützen. Wie Sie das Firmwarepaket aktualisieren und die Softwareversion überprüfen, können Sie dem Konfigurationsleitfaden für Ihre Software entnehmen. Weitere Informationen finden Sie im [Cisco Secure Firewall Threat Defense-Kompatibilitätsleitfaden](#) und im [Cisco Secure Firewall ASA-Kompatibilitätsleitfaden](#). Diese enthalten Informationen zur Kompatibilität der Software und Hardware jeder unterstützten Cisco Version, einschließlich Anforderungen an Betriebssystem und Hosting-Umgebung.

Die folgende Abbildung zeigt die Vorderseite des 1000Base-T-Netzwerkmoduls mit 8 Ports.



Hinweis Wenn ein Port im 400-Gbit/s-, 200-Gbit/s-, 100-Gbit/s- oder 40-Gbit/s-Modus betrieben wird, zeigt nur die obere LED des Ports den Verbindungs-/Aktivitätsstatus an.

Abbildung 13: CSF6K-XNM-8X1GF



1	Umgehungs-LEDs B1 bis B4 <ul style="list-style-type: none"> • Grün: Im Standby-Modus. • Orange blinkend: Der Port befindet sich im Hardwareumgehungsmodus; Fehlerereignis. 	2	Ethernet 2/1 und 2/2 oder Ethernet 3/1 und 3/2 Die Ports 1 und 2 werden gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden. Die LED B1 gilt für diesen gekoppelten Port.
----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3	Ethernet 2/3 und Ethernet 2/4 oder Ethernet 3/3 und 3/4 Die Ports 3 und 4 sind gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden. Die LED B2 gilt für diesen gekoppelten Port.	4	Ethernet 2/5 und 2/6 oder Ethernet 3/5 und 3/6 Die Ports 5 und 6 sind gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden. Die LED B3 gilt für diesen gekoppelten Port.
5	Ethernet 2/7 und 2/8 oder Ethernet 3/7 und 3/8 Die Ports 7 und 8 werden gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden. Die LED B4 gilt für diesen gekoppelten Port.	6	Unverlierbare Schraube
7	Betriebsanzeige-LED	8	Griff
9	Linke Port-LED <ul style="list-style-type: none"> • Aus: Keine Verbindung oder Port nicht verwendet. • Grün: Verbindung aktiv. • Grün blinkend: Netzwerkaktivität. 	10	Rechte Port-LED <ul style="list-style-type: none"> • Aus: Keine Verbindung oder Port nicht verwendet. • Grün: Verbindung aktiv. • Grün blinkend: Netzwerkaktivität.

6-Port-Netzwerkmodul mit 1 Gbit/s SX/10-Gbit/s SR/10-Gbit/s LR/25-Gbit/s SR/25-Gbit/s LR mit Hardware-Umgehung (CSF6K-XNM-6X10SRF, CSF6K-XNM-6X10LRF, CSF6K-XNM-6X25SRF und CSF6K-XNM-6X25LRF)

Unter [Unterstützte Transceiver, auf Seite 33](#) finden Sie die Softwareversion und die Transceiver-Unterstützung für dieses Netzwerkmodul.

Das Chassis der Secure Firewall 6100 verfügt über zwei Netzwerkmodul-Steckplätze mit den Bezeichnungen NM-2 und NM-3 (von links nach rechts an der Vorderseite). Netzwerkmodule sind optionale, herausnehmbare I/O-Module, die entweder zusätzliche Ports oder verschiedene Schnittstellentypen bereitstellen. Das Netzwerkmodul wird auf der Vorderseite des Chassis angeschlossen. Unter [Vorderseite, auf Seite 8](#) finden Sie Informationen zur Position der Netzwerkmodul-Steckplätze am Chassis.

Die Netzwerkmodule CSF6K-XNM-6X10SRF, CSF6K-XNM-6X10LRF, CSF6K-XNM-6X25SRF und CSF6K-XNM-6X25LRF mit Hardwareumgehung verfügen über sechs Ports, die von oben nach unten und von links nach rechts nummeriert sind. Koppeln Sie die Ports 1 und 2, 3 und 4 sowie 5 und 6, um einen gekoppelten Schnittstellensatz mit Hardwareumgehung zu bilden. Im Hardwareumgehungsmodus werden die Daten nicht von der Secure Firewall 6100 verarbeitet, sondern an den gekoppelten Port weitergeleitet. Dieses Netzwerkmodul verfügt über integrierte SFP-Transceiver. Hot Swap und Vor-Ort-Austausch der Transceiver werden nicht unterstützt.

Eine Hardwareumgehung (auch bekannt als Fail-to-Wire) ist eine Umgehung für eine physische Schicht (Layer 1), die den Wechsel gekoppelter Schnittstellen in den Umgehungsmodus erlaubt, damit die Hardware

Pakete zwischen diesen Port-Paaren ohne Softwareeingriff weiterleitet. Eine Hardwareumgehung ermöglicht Netzwerkverbindungen, wenn Software- oder Hardwarefehler auftreten. Die Hardwareumgehung ist nützlich für Ports, bei denen die Cisco Secure Firewall den Datenverkehr nur überwacht oder protokolliert. Netzwerkmodule mit Hardwareumgehung verfügen über einen Switch, der die beiden Ports bei Bedarf verbinden kann. Dieses Netzwerkmodul mit Hardwareumgehung verfügt über integrierte SFPs.



Hinweis Die Hardwareumgehung wird nur bei Threat Defense unterstützt, Sie können diese Module jedoch auch im Nichtumgehungsmodus in Threat Defense oder ASA verwenden.

Die Hardwareumgehung wird nur auf festgelegten Ports unterstützt. Sie können Port 1 mit Port 2 und Port 3 und Port 4 koppeln; Sie können allerdings Port 1 nicht mit Port 4 koppeln.



Hinweis Wenn die Appliance vom normalen Betrieb zur Hardwareumgehung oder von der Hardwareumgehung zurück in den normalen Betrieb wechselt, kann der Datenverkehr für mehrere Sekunden unterbrochen werden. Eine Reihe von Faktoren kann sich auf die Dauer der Unterbrechung auswirken: das Verhalten des Verbindungspartners und seine Art und Weise, wie er Verbindungsfehler und die Zeitüberschreitung für das Entprellen handhabt; die Spanning Tree Protocol-Konvergenz; die Konvergenz des dynamischen Routing-Protokolls usw. Während dieser Zeit kann es zu Verbindungsunterbrechungen kommen.



Hinweis Wenn Sie einen Inline-Schnittstellensatz mit einer Kombination aus Schnittstellen mit und ohne Hardwareumgehung haben, können Sie die Hardwareumgehung für diesen Inline-Schnittstellensatz nicht aktivieren. Sie können die Hardwareumgehung für einen Inline-Schnittstellensatz nur aktivieren, wenn alle Paare im Inline-Schnittstellensatz gültige Sätze mit Hardwareumgehung sind.



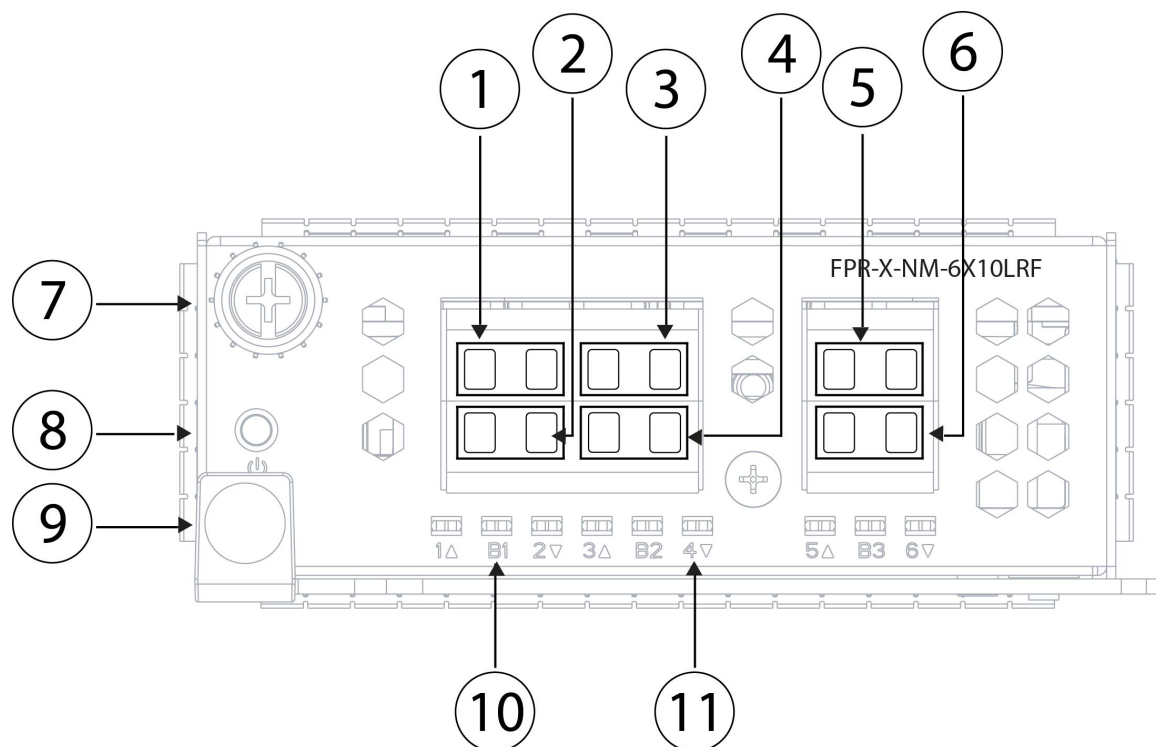
Hinweis Die Hardware und das System unterstützen den Austausch im laufenden Betrieb (Hot Swap), wenn Sie ein Netzwerkmodul durch ein Netzwerkmodul desselben Typs ersetzen. Wenn Sie das 10/25-Gbit/s-Netzwerkmodul mit 6 Ports durch ein anderes unterstütztes Netzwerkmodul ersetzen, müssen Sie das Chassis neu starten, damit das neue Netzwerkmodul erkannt wird. Weitere Informationen zum Management von Netzwerkmodulen finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.



Hinweis Stellen Sie sicher, dass Sie das richtige Firmwarepaket und die richtige Softwareversion installiert haben, um dieses Netzwerkmodul zu unterstützen. Wie Sie ermitteln können, welches Firmwarepaket und welche Softwareversion vorliegen, können Sie dem Konfigurationsleitfaden für Ihre Software entnehmen. Weitere Informationen finden Sie im [Cisco Secure Firewall Threat Defense-Kompatibilitätsleitfaden](#) und im [Cisco Secure Firewall ASA-Kompatibilitätsleitfaden](#). Diese enthalten Informationen zur Kompatibilität der Software und Hardware jeder unterstützten Cisco Version, einschließlich Anforderungen an Betriebssystem und Hosting-Umgebung.

Die folgende Abbildung zeigt die Vorderseite des 1/10/25 Gbit/s-Netzwerkmoduls mit 6 Ports.

Abbildung 14: CSF6K-XNM-6X10SRF, CSF6K-XNM-6X10LRF, CSF6K-XNM-6X25SRF und CSF6K-XNM-6X25LRF



1	Port 1 Ethernet 2/1 oder 3/1 Die Ports 1 und 2 werden gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden.	2	Port 2 Ethernet 2/2 oder 3/2 Die Ports 1 und 2 werden gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden.
3	Port 3 Ethernet 2/3 oder 3/3 Die Ports 3 und 4 sind gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden.	4	Port 4 Ethernet 2/4 oder 3/4 Die Ports 3 und 4 sind gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden.
5	Port 5 Ethernet 2/5 oder 3/5 Die Ports 5 und 6 sind gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden.	6	Port 6 Ethernet 2/6 oder 3/6 Die Ports 5 und 6 sind gekoppelt, um einen Schnittstellensatz mit Hardwareumgehung zu bilden.
7	Unverlierbare Schraube	8	Betriebsanzeige-LED

9	Auswurfhebel	10	Umgehungs-LEDs B1 bis B3: <ul style="list-style-type: none"> • Aus: Der Umgehungsmodus ist deaktiviert. • Grün: Der Port befindet sich im Standby-Modus. • Orange blinkend: Der Port befindet sich im Hardwareumgehungsmodus; Fehlerereignis.
11	Sechs Netzwerkaktivitäts-LEDs: <ul style="list-style-type: none"> • Orange: Keine Verbindung, Port wird nicht verwendet, keine Verbindung oder Netzwerkfehler. • Grün: Verbindung ist aktiv, keine Netzwerkaktivität. • Grün blinkend: Netzwerkaktivität. 	—	

Netzstrommodule

Die Secure Firewall 6100 unterstützt zwei AC- oder DC-Netzteilmodule, sodass ein redundanter Schutz durch zwei Netzteile möglich ist. Die Netzteilmodule sind zur Rückseite des Chassis ausgerichtet und sind von oben nach unten durchnummeriert: PSU-1 und PSU-2.

Das Netzteilmodul ist Hot-Swap-fähig. Eine Liste der PIDs im Zusammenhang mit den Netzteilmodulen der Secure Firewall 6100 finden Sie unter [Produkt-IDs, auf Seite 50](#).



Hinweis Nachdem Sie das Chassis von der Stromversorgung getrennt haben, warten Sie mindestens 10 Sekunden, bevor Sie die Stromversorgung wieder einschalten. Lassen Sie das System, einschließlich der Standby-Stromversorgung, 10 Sekunden lang ausgeschaltet.



Achtung Stellen Sie sicher, dass ein Netzteilmodul immer aktiv ist.

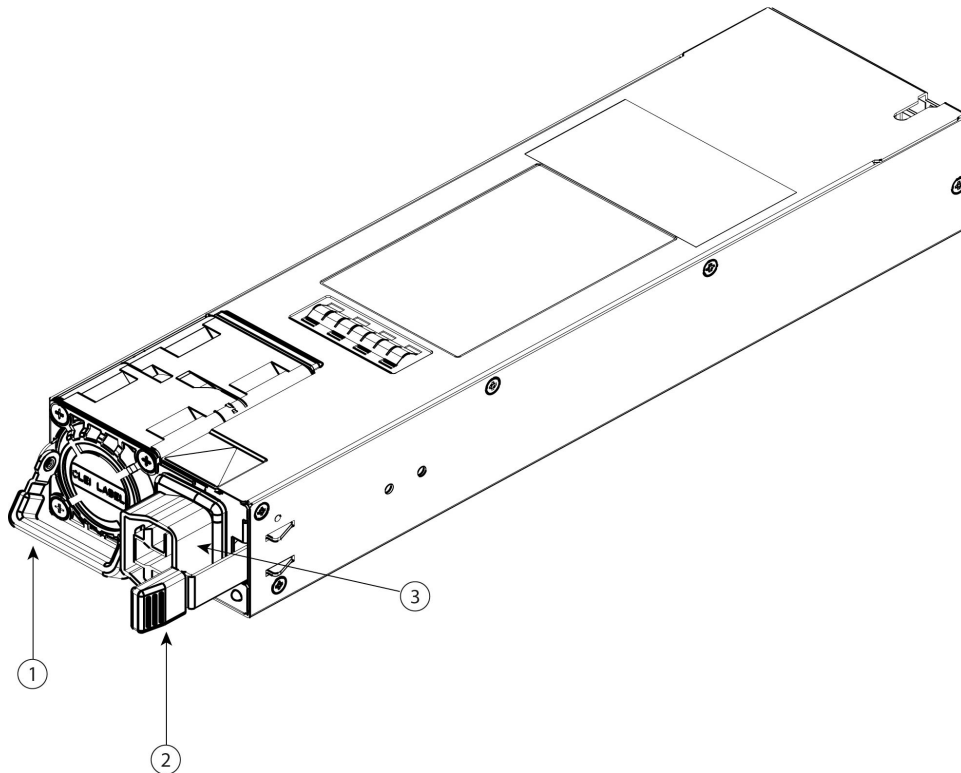
Das CSF6100-PWR-AC-Netzteil hat einen Dreifacheingang: AC (Hochbereich), HVAC (Hochbereich) und HVDC. Die doppelten Netzteile können bis zu 3.000 W Leistung im gesamten Eingangsspannungsbereich (220 VAC) erzeugen. Die Last wird aufgeteilt, wenn beide Netzteilmodule eingesteckt sind und gleichzeitig betrieben werden.

Das HVAC/HVDC-Netzteilmodul kann mit einer Eingangsspannung von 110 VAC (Niedrigbereich) betrieben werden, die Ausgangsleistung wird jedoch auf die Hälfte reduziert (jeweils 1.500 W). Mit zwei installierten Netzteilmodulen kann das System eine Leistung von 3.000 W erreichen, aber Redundanz ist nicht verfügbar.



Hinweis Das System verbraucht nicht mehr als die Kapazität eines Netzteilmoduls und wird somit immer vollständig im Redundanzmodus betrieben, wenn zwei Netzteilmodule installiert sind.

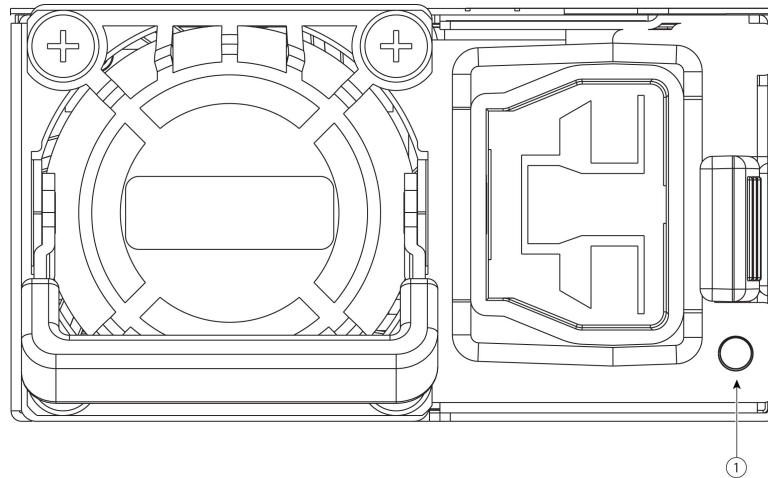
Abbildung 15: Netzteilmodul



1	Griff	2	Arretierlasche
3	Netzkabelanschluss		—

Die folgende Abbildung zeigt die zweifarbige LED des Netzteils am Netzteilmodul.

Abbildung 16: Netzteilmodul-LED



1	<p>Netzteil-LED:</p> <ul style="list-style-type: none"> • Grün: Aktiver Modus • Grün, blinkend: Standby-Modus • Grün, blinkend: Boot-Ladevorgang • Orange: Kein Wechselstrom, aber das andere Netzteilmodul im System ist in Betrieb • Orange blinkend: Warnereignis (hohe Temperatur oder Lüfterausfall) • Aus: Keine Eingangsspannung
----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Weitere Informationen

- Unter [Entfernen und Austauschen des Netzteilmoduls, auf Seite 94](#) finden Sie die Vorgehensweise für den Ausbau und Austausch des Netzteilmoduls bei der Cisco Secure Firewall 6100.

Lüftermodule

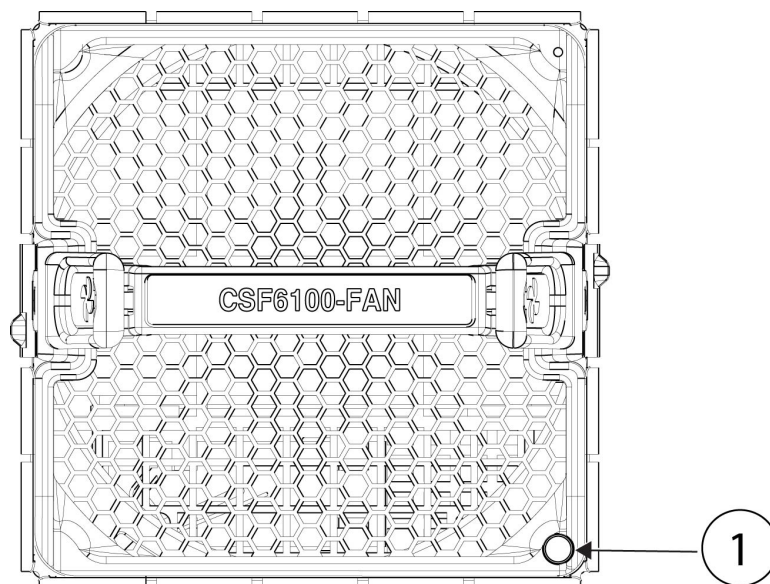
Die Secure Firewall 6100-Serie ist mit vier axialen Doppelrotor-Lüftermodulen ausgestattet. Wenn ein Lüfter ausfällt, drehen die anderen Lüftermodule mit maximaler Geschwindigkeit, damit das System weiterhin funktioniert. Die Lüftermodule sind im laufenden Betrieb austauschbar (Hot Swap) und werden auf der Rückseite des Chassis installiert. Sie sind von links nach rechts auf der Rückseite des Chassis mit FAN-1 bis FAN-4 gekennzeichnet.



Vorsicht Wenn ein Lüftermodul ausfällt, entfernen Sie es aus dem Chassis und ersetzen Sie es innerhalb von 30 Sekunden. Nach 30 Sekunden kann die CPU-Temperatur die Betriebstemperatur überschreiten, was die Leistung beeinträchtigen kann. Unter [Entfernen und Austauschen des Lüftermoduls, auf Seite 92](#) finden Sie die Vorgehensweise zum Entfernen und Austauschen des Lüftermoduls.

In der folgenden Abbildung ist die Position der Lüfter-LED am Lüftermodul dargestellt.

Abbildung 17: Lüftermodul-LED



1	Zweifarbige LED (Grün und Gelb)
----------	---------------------------------

Das Lüftermodul verfügt über eine zweifarbige LED, die sich in der oberen linken Ecke des Lüfters befindet.

- Aus: Keine Stromversorgung oder das System wird hochgefahren.
- Grün: Lüfter laufen normal. Es kann nach dem Start bis zu eine Minute dauern, bis die LED grün wird.
- Gelb, blinkend: Die Drehzahl von einem oder mehreren Lüfterrotoren weicht von der Norm ab. Dies erfordert sofortige Aufmerksamkeit.
- Gelb: Ein oder mehrere Lüfter sind ausgefallen. Das System kann weiterhin normal betrieben werden, aber der Lüfter muss gewartet werden.

Weitere Informationen

- Eine Liste der PIDs im Zusammenhang mit den Lüftern der Secure Firewall 6100-Serie finden Sie unter [Produkt-IDs, auf Seite 50](#).
- Unter [Entfernen und Austauschen des Lüftermoduls, auf Seite 92](#) wird Vorgehensweise zum Entfernen und Austauschen des Lüftermoduls beschrieben.

SSDs

Die Secure Firewall 6100-Serie verfügt über zwei SSD-Steckplätze, die jeweils eine NVMe-SSD (Non-Volatile Memory Express) aufnehmen. Die Secure Firewall 6160-Serie wird standardmäßig mit zwei 3,6-TB-SSDs in den Steckplätzen 1 und 2 ausgeliefert. Die Secure Firewall 6170 wird mit zwei 7,2-TB-SSDs in den Steckplätzen 1 und 2 ausgeliefert. Die Software RAID1 wird bereits konfiguriert ausgeliefert.

Hot Swap wird unterstützt. Sie können SSDs austauschen, ohne das Chassis auszuschalten. Sie müssen jedoch vor dem Hot-Swap von SSDs den Befehl **raid remove-secure local-disk 1|2** ausführen, um die SSD auf den

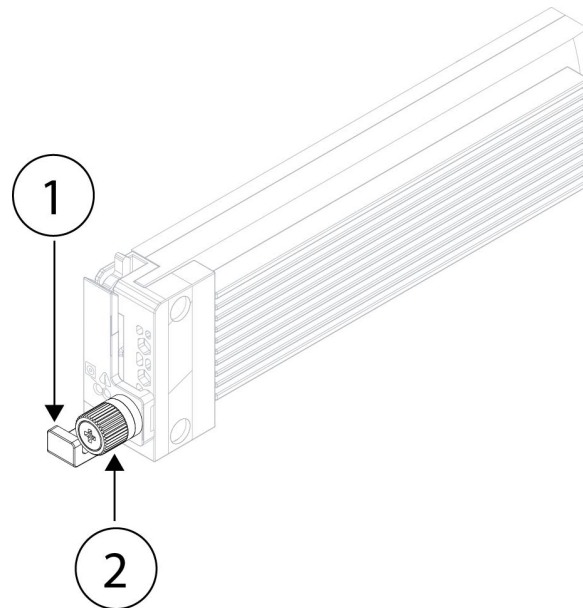
Austausch vorzubereiten. Mit diesem Befehl werden die Daten auf der SSD beibehalten. Nachdem Sie die SSD entfernt und ausgetauscht haben, müssen Sie sie anschließend mit dem Befehl **raid add local-disk 1|2** erneut zur RAID1-Konfiguration hinzufügen. Unter [Hot-Swapping einer SSD auf der Cisco Secure Firewall 3100/4200](#) finden Sie die Verfahren zum sicheren Entfernen einer SSD.



Vorsicht Der Befehl **raid remove-secure local disk** ermöglicht das sichere Löschen der angegebenen SSD-Daten.

Eine Liste der PIDs im Zusammenhang mit den SSDs der Secure Firewall 6100-Serie finden Sie unter [Produkt-IDs, auf Seite 50](#). Die IDs der SSD-Laufwerke lauten `disk0:` und `disk1:`.

Abbildung 18: SSD



1	SSD-Arretierlasche	2	Unverlierbare Schraube
---	--------------------	---	------------------------

Weitere Informationen

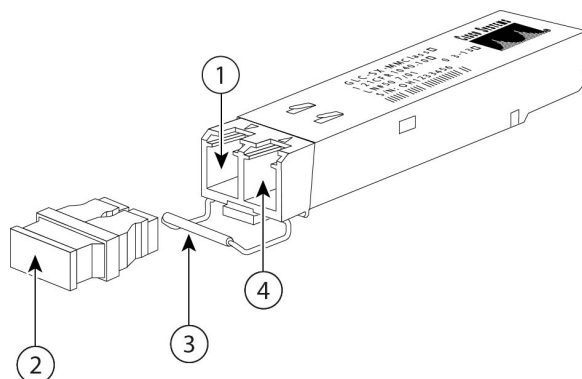
- Unter [LEDs an der Vorderseite](#), auf Seite 12 finden Sie die Position und die Beschreibung der SSD-LEDs auf der Vorderseite.
- Unter [Entfernen und Austauschen der SSD](#), auf Seite 91 finden Sie die Vorgehensweise für den Ausbau und den Austausch einer SSD.
- Im Konfigurationsleitfaden für Ihre Software finden Sie die Verfahren zum Entfernen und Hinzufügen einer SSD aus der bzw. zur RAID1-Konfiguration.

Unterstützte Transceiver

Der Transceiver ist ein bidirektionales Gerät, bei dem sich Sender und Empfänger im selben Gehäuse befinden. Es ist eine im laufenden Betrieb austauschbare optische oder elektrische (Kupfer-)Schnittstelle, die an die

SFP/QSFP/QSFP-DD-Ports an den fest konfigurierten Ports und den Ports der Netzwerkmodule angeschlossen wird und Ethernet-Verbindungen ermöglicht.

Abbildung 19: SFP-Transceiver



1	Staubschutzkappe	2	Verschluss
3	Optischer Anschluss (Empfangen)	4	Optischer Anschluss (Senden)

Sicherheitswarnungen

Beachten Sie die folgenden Warnhinweise:



Warnung Anweisung 1055 – Laser der Klasse 1/1M

Unsichtbare Laserstrahlung ist vorhanden. Setzen Sie BenutzerInnen von Teleskopoptiken keinem Risiko aus. Dies gilt für Laserprodukte der Klasse 1/1M.



Warnung Anweisung 1056 – Nicht abgeschlossenes Glasfaserkabel

Von nicht abgeschlossenen Faserkabeln oder Anschlüssen kann unsichtbare Laserstrahlung ausgehen. Blicken Sie nicht direkt mit optischen Instrumenten darauf. Das Betrachten des Laserausgangs mit bestimmten optischen Geräten (Lupen, Vergrößerungsgläser, Mikroskop usw.) in einem Abstand von 100 mm kann zu Augenschäden führen.



Warnung Anweisung 1057 – Freisetzung gefährlicher Strahlung

Die Verwendung von Kontrollen, Anpassungen oder die Durchführung von Verfahren, die sich von den hier angegebenen unterscheiden, kann/können zur Freisetzung gefährlicher Strahlung führen.

**Warnung**

Wenden Sie beim Einlegen des Transceivers geeignete Schutzmaßnahmen gegen elektrostatische Entladungen (ESD) an. Vermeiden Sie es, die Kontakte auf der Rückseite zu berühren, und halten Sie die Kontakte und Ports frei von Staub und Schmutz. Bewahren Sie ungenutzte Transceiver zum Schutz vor elektrostatischer Entladung in der Verpackung auf, in der sie versendet wurden.

**Vorsicht**

SFP anderer Hersteller sind zwar zulässig, aber wir empfehlen deren Verwendung nicht, da sie nicht von Cisco getestet und validiert wurden. Cisco TAC kann den Support für jegliche Interoperabilitätsprobleme verweigern, die aus der Verwendung eines ungetesteten Dritt-SFP-Transceivers hervorgehen.

In der folgenden Tabelle sind die SFPs aufgeführt, die an den fest konfigurierten Ports der Secure Firewall 6160 und 6170 unterstützt werden.

Tabelle 2: CSF6160 und CSF6170 – fest konfigurierte Ports

Port-Typ	Transceiver-PID	Erste unterstützte Version
Feste konfigurierte SFP/SFP+/SFP28-Ports		Threat Defense 10.0/ASA 9.24

Port-Typ	Transceiver-PID	Erste unterstützte Version
	<ul style="list-style-type: none"> • GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-GE-100FX • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-10G-TX • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM • SFP-25G-SR-S • SFP-10/25G-CSR-S • SFP-10/25G-LR-S • SFP-H25-CUxM • SFP-25G-AOCxM • SFP-50G-CUxM • SFP-50G-SL • SFP-50G-SR-S • SFP-50G-LR-S • QSFP-40G-SR4 • QSFP-40G-SR4-S • QSFP-40G-CSR4 • QSFP-40G-SR-BD • QSFP-40G-LR4 • QSFP-40G-LR4-S 	

Port-Typ	Transceiver-PID	Erste unterstützte Version
	<ul style="list-style-type: none"> • WSP-Q40GLR4L • QSFP-H40G-CUxM • QSFP-H40G-ACUxM • QSFP-4SFP10G-CUxM • QSFP-4X10G-ACxM • QSFP-H40G-AOCxM • QSFP-4X10G-AOCxM • QSFP-100G-SR4-S • QSFP-100G-LR4-S • QSFP-100G-LR-S • QSFP-100G-AOCxM • QSFP-100G-CUxM • QSFP-4SFP25G-CUxM • QSFP-100G-FR-S • QSFP-100G-SM-SR • QSFP-100G-SR1.2 • QSFP-100G-DR-S • QSFP-40/100-SRBD • QSFP-200-CU3M • QSFP-200G-SR4-S • QSFP-200G-SL4 • QSFP-200G-FR4-S • QDD-2Q200-CU3M • QDD-2X100-LR4-S • QDD-2X100-SR4-S 	

In der folgenden Tabelle sind die SFPs aufgeführt, die an den Management-Ports der Secure Firewall 6160 und 6170 unterstützt werden.

Tabelle 3: CSF6160 und CSF6170 – Management-Ports

Port-Typ	Transceiver-PID	Erste unterstützte Version
Management-SFP/SFP+/SFP28-Ports	<ul style="list-style-type: none"> • GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-10G-TX • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM • SFP-25G-SR-S • SFP-10/25G-CSR-S • SFP-10/25G-LR-S • SFP-H25-CUxM • SFP-25G-AOCxM 	Threat Defense 10.0/ASA 9.24

In der folgenden Tabelle sind die SFPs aufgeführt, die auf dem 10 Gbit/s-Netzwerkmodul mit 8 Ports unterstützt werden.

Tabelle 4: CSF6160 und CSF6170 – 10-Gbit/s-Netzwerkmodul mit 8 Ports

Port-Typ	Transceiver-PID	Erste unterstützte Version
CSF6K-XNM-8X10G	<ul style="list-style-type: none"> • GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-10G-TX • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM 	Threat Defense 10.0/ASA 9.24

In der folgenden Tabelle sind die SFPs aufgeführt, die auf dem 25 Gbit/s-Netzwerkmodul mit 8 Ports unterstützt werden.

Tabelle 5: CSF6160 und CSF6170 – 25-Gbit/s-Netzwerkmodul mit 8 Ports

Port-Typ	Transceiver-PID	Erste unterstützte Version
CSF6K-XNM-8X25G	<ul style="list-style-type: none"> • GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-10G-TX • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM • SFP-25G-SR-S • SFP-10/25G-CSR-S • SFP-10/25G-LR-S • SFP-H25-CUxM • SFP-25G-AOCxM 	Threat Defense 10.0/ASA 9.24

In der folgenden Tabelle sind die SFPs aufgeführt, die auf dem 40-Gbit/s-Netzwerkmodul mit 4 Ports unterstützt werden.

Tabelle 6: CSF6160 und CSF6170 – 40-Gbit/s-Netzwerkmodul mit 4 Ports

Port-Typ	Transceiver-PID	Erste unterstützte Version
CSF6K-XNM-4X40G	<ul style="list-style-type: none"> • QSFP-40G-SR4 • QSFP-40G-SR4-S • QSFP-40G-CSR4 • QSFP-40G-SR-BD • QSFP-40G-LR4-S • QSFP-40G-LR4 • WSP-Q40GLR4L • QSFP-H40G-CUxM • QSFP-H40G-ACUxM • QSFP-4SFP10G-CUxM • QSFP-4X10G-ACxM • QSFP-H40G-AOCxM • QSFP-4X10G-AOCxM 	Threat Defense 10.0/ASA 9.24

In der folgenden Tabelle sind die SFPs aufgeführt, die auf dem 100-Gbit-/s-Netzwerkmodul mit 2 Ports unterstützt werden.

Tabelle 7: CSF6160 und CSF6170 – 100-Gbit/s-Netzwerkmodul mit 2 Ports

Port-Typ	Transceiver-PID	Erste unterstützte Version
CSF6K-XNM-2X100G	<ul style="list-style-type: none"> • QSFP-40G-SR4 • QSFP-40G-SR4-S • QSFP-40G-CSR4 • QSFP-40G-SR-BD • QSFP-40G-LR4 • QSFP-40G-LR4-S • WSP-Q40GLR4L • QSFP-H40G-CUxM • QSFP-H40G-ACUxM • QSFP-4SFP10G-CUxM • QSFP-4X10G-ACxM • QSFP-H40G-AOCxM • QSFP-4X10G-AOCxM • QSFP-100G-SR4-S • QSFP-100G-LR4-S • QSFP-40/100G-SRBD • QSFP-100G-LR-S • QSFP-100G-AOCxM • QSFP-100G-CUxM • QSFP-4SFP25G-CUxM • QSFP-100G-FR-S • QSFP-100G-SM-SR • QSFP-100G-SR1.2 • QSFP-100G-DR-S 	Threat Defense 10.0/ASA 9.24

In der folgenden Tabelle sind die SFPs aufgeführt, die auf dem 200-Gbit/s-Netzwerkmodul mit 4 Ports unterstützt werden.

Tabelle 8: FPCAF6160 und CSF6170 – 200-Gbit/s-Netzwerkmodul mit 4 Ports

Port-Typ	Transceiver-PID	Erste unterstützte Version
CSF6K-XNM-4X200G		Threat Defense 10.0/ASA 9.24

Port-Typ	Transceiver-PID	Erste unterstützte Version
	<ul style="list-style-type: none"> • QSFP-40G-SR4 • QSFP-40G-SR4-S • QSFP-40G-CSR4 • QSFP-40G-SR-BD • QSFP-40G-LR4 • QSFP-40G-LR4-S • WSP-Q40GLR4L • QSFP-H40G-CUxM • QSFP-H40G-ACUxM • QSFP-4SFP10G-CUxM • QSFP-4X10G-ACxM • QSFP-H40G-AOCxM • QSFP-4X10G-AOCxM • QSFP-100G-SR4-S • QSFP-100G-LR4-S • QSFP-40/100G-SRBD • QSFP-100G-LR-S • QSFP-100G-AOCxM • QSFP-100G-CUxM • QSFP-4SFP25G-CUxM • QSFP-100G-FR-S • QSFP-100G-SM-SR • QSFP-100G-SR1.2 • QSFP-100G-DR-S • QSFP-200-CU3M • QSFP-200G-SR4-S • QSFP-200G-SL4 • QSFP-200G-FR4-S • QDD-2Q200-CU3M • QDD-2X100-LR4-S • QDD-2X100-SR4-S 	

In der folgenden Tabelle sind die SFPs aufgeführt, die auf dem 400-Gbit/s-Netzwerkmodul mit 2 Ports unterstützt werden.

Tabelle 9: CSF6160 und CSF6170 – 400-Gbit/s-Netzwerkmodul mit 2 Ports

Port-Typ	Transceiver-PID	Erste unterstützte Version
CSF6K-XNM-2X400G		Threat Defense 10.0/ASA 9.24

Port-Typ	Transceiver-PID	Erste unterstützte Version
	<ul style="list-style-type: none"> • QSFP-40G-SR4 • QSFP-40G-SR4-S • QSFP-40G-CSR4 • QSFP-40G-SR-BD • QSFP-40G-LR4 • QSFP-40G-LR4-S • WSP-Q40GLR4L • QSFP-H40G-CUxM • QSFP-H40G-ACUxM • QSFP-4SFP10G-CUxM • QSFP-4X10G-ACxM • QSFP-H40G-AOCxM • QSFP-4X10G-AOCxM • QSFP-100G-SR4-S • QSFP-100G-LR4-S • QSFP-40/100G-SRBD • QSFP-100G-LR-S • QSFP-100G-AOCxM • QSFP-100G-CUxM • QSFP-4SFP25G-CUxM • QSFP-100G-FR-S • QSFP-100G-SM-SR • QSFP-100G-SR1.2 • QSFP-100G-DR-S • QSFP-200-CU3M • QSFP-200G-SR4-S • QSFP-200G-SL4 • QDD-2Q200-CU3M • QDD-2X100-LR4-S • QDD-2X100-SR4-S • QDD-400G-DR4-S 	

Port-Typ	Transceiver-PID	Erste unterstützte Version
	<ul style="list-style-type: none"> • QDD-4x100G-FR-S • QDD-4x100G-LR-S • QDD-400G-SR4.2-BD • QDD-400G-FR4-S • QDD-400G-LR4-S • QDD-400-CUxM • QDD-400-AOCxM • QDD-4ZQ100-CU3M 	

Hardwarespezifikationen

In der folgenden Tabelle sind die Hardwarespezifikationen für die Cisco Secure Firewall 6100-Serie aufgelistet.

Tabelle 10: Hardwarespezifikationen für CSF-6160 und CSF-6170

Spezifikation	CSF-6160	CSF-6170
Chassis		
Chassis-Abmessungen (H x B x T)	8,89 x 42,926 x 82,55 cm (3,5 x 16,9 x 32,5 Zoll)	
Netzwerkmodulabmessungen (H x B x T)	3,58 x 9,3 x 25,25 cm (1,41 x 3,66 x 9,94 Zoll)	
Chassis-Gewicht (vollständig bestückt)	29,93 kg (66 lb)	
Stromversorgung		
Abmessungen des Netzteilmoduls	40,0 x 67,5 x 252 mm (1,575 x 2,657 x 9,92 Zoll)	
Konfiguration	2 Netzteilmodule; jeweils bis zu 3.000 W, Hot-Swap-fähig, Redundanz mit Lastverteilung	
Eingangsspannung (Wechselstrom)	100 bis 120 VAC (HVAC, Niedrigbereich) 200 bis 277 VAC (HVAC, Hochbereich)	
AC-Eingangsfrequenz	50 bis 60 Hz (nominal)	
HVDC-Eingangsspannung	240 bis 380 VDC	
LVDC-Eingangsspannung	-48 bis -60 VDC	
AC-Stromaufnahme (maximal)	13 A (Hochbereich Wechselstrom)	14 A (Hochbereich Wechselstrom)

Spezifikation	CSF-6160	CSF-6170
System-HVDC-Stromaufnahme (maximal)	11 A	12 A
System-LVDC-Stromaufnahme (maximal)	29 A	33 A
Leistungsaufnahme	1.740 W (typisch) 2.440 W (maximal)	2.010 W (typisch) 2.760 W (maximal)
Umgebungsbedingungen		
Temperatur	Betrieb: 0 bis 40 °C (32 bis 104 °F) Bei einer Einsatzhöhe über 1800 m verringert sich die maximale Betriebstemperatur um 1 °C pro 300 m. Ruhezustand: -40 bis 65 °C (-40 bis 149 °F)	Betrieb: 10 bis 35 °C (50 bis 95 °F) Bei einer Einsatzhöhe über 1800 m verringert sich die maximale Betriebstemperatur um 1 °C pro 300 m. Ruhezustand: -40 bis 65 °C (-40 bis 149 °F)
Luftfeuchtigkeit	Betrieb: 5–90 %, nicht kondensierend Ruhezustand: 5 bis 95 %, nicht kondensierend	
Höhenlage	Betrieb: 0 bis 3,048 m (0 bis 10.000 ft) Betrieb: 0 bis 2.000 m (0 bis 6.562 ft) in China Bei einer Einsatzhöhe über 1.828 m (6.000 ft) verringert sich die maximale Betriebstemperatur um 1 °C pro 304 m (1.000 ft). Ruhezustand: maximal 12.192 m (40.000 ft)	
Schalldruck	≤ 74 dBa (Standard) ≤ 90 dBa (maximal) Hinweis Dieses System kann 85 dBA überschreiten, wenn es in Umgebungen mit hoher Umgebungstemperatur betrieben wird. In Umgebungen über 85 dBA ist ein Gehörschutz gegen Schalldruck erforderlich.	
Schallleistung	≤ 81 dB (Standard) ≤ 98 dB (maximal)	

Produkt-IDs

In der folgenden Tabelle sind die Produkt-IDs (PIDs) für die Secure Firewall 6100-Serie aufgeführt. Alle PIDs in der Tabelle sind vor Ort austauschbar. Wenn Sie eine RMA (Return Material Authorization) für eine Komponente benötigen, finden Sie weitere Informationen im [Cisco Retourenportal](#).



Hinweis Verwenden Sie den Befehl **show inventory** aus der [Befehlsreferenz zu Cisco Secure Firewall Threat Defense](#) oder der [Befehlsreferenz zur Cisco ASA-Serie](#), um eine Liste mit PIDs für die Secure Firewall 6100-Serie anzuzeigen.

Table 11: CSF-6160 und CSF-6170 – PIDs

PID	Beschreibung
Chassis	
CSF6160-A-ASA-K9	Secure Firewall 6160 Appliance, ASA
CSF6170-A-ASA-K9	Secure Firewall 6170 Appliance, ASA
CSF6160-A-TD-K9	Secure Firewall 6160 Appliance, Threat Defense
CSF6170-A-TD-K9	Secure Firewall 6170 Appliance, Threat Defense
Modulare Komponenten	
CSF6100-PWR-AC	AC/HVAC/HVDC-Netzteil
CSF6100-PWR-AC=	AC/HVAC/HVDC-Netzteil (Ersatzteil)
CSF6100-FAN	Lüftermodul
CSF6100-FAN=	Lüftermodul (Ersatzteil)
CSF6100-SSD3600	SSD-Modul für die Secure Firewall 6160
CSF6100-SSD3600=	SSD-Modul für die Secure Firewall 6160 (Ersatzteil)
CSF6100-SSD7200	SSD-Modul für die Secure Firewall 6170
CSF6100-SSD7200=	SSD-Modul für die Secure Firewall 6170 (Ersatzteil)
Arbeitsspeicher	
CSF6100-MEM-C1X64-	Secure Firewall 6160 CPU – 1 x 64 GB
CSF6100-MEM-C1X96-	Secure Firewall 6170 CPU – 1 x 96 GB
Kits	
CSF6100-ACC-KIT	Hardware-Zubehör-Kit (Rackmontage, Kabel)
CSF6100-ACC-KIT=	Hardware-Zubehör-Kit (Rackmontage, Kabel) (Ersatzteil)
CSF6100-MEM-C1X64=	Secure Firewall 6160 CPU – Arbeitsspeicher-Kit mit 1 x 64 GB (Ersatzteil)

PID	Beschreibung
CSF6100-MEM-C1X96=	Secure Firewall 6170 CPU – Arbeitsspeicher-Kit mit 1 x 96 GB (Ersatzteil)
CSF6100-SLD-RAILS	Gleitschienen-Satz
CSF6100-SLD-RAILS=	Gleitschienen-Satz (Ersatzteil)
CSF6100-CBL-MGMT	Kabelmanagement-Halteklammern
CSF6100-CBL-MGMT=	Kabelmanagement-Halteklammern (Ersatzteil)
Netzwerkmodule	
CSF6K-XNM-6X1SXF	1-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, SX-Multimode
CSF6K-XNM-6X1SXF=	1-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, SX-Multimode (Ersatzteil)
CSF6K-XNM-6X10SRF	10-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, SR-Multimode
CSF6K-XNM-6X10SRF=	10-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, SR-Multimode (Ersatzteil)
CSF6K-XNM-6X10LRF	10-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, LR-Singlemode
CSF6K-XNM-6X10LRF=	10-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, LR-Singlemode (Ersatzteil)
CSF6K-XNM-6X25SRF	25-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, SR-Multimode
CSF6K-XNM-6X25SRF=	25-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, SR-Multimode (Ersatzteil)
CSF6K-XNM-6X25LRF	25-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, LR-Singlemode
CSF6K-XNM-6X25LRF=	25-Gbit/s-SFP-Netzwerkmodul mit Hardwareumgehung und 6 Ports, LR-Singlemode (Ersatzteil)
CSF6K-XNM-8X1GF	10/100/1000Base-10-Netzwerkmodul mit Hardwareumgehung und 8 Ports
CSF6K-XNM-8X1GF=	10/100/1000Base-10-Netzwerkmodul mit Hardwareumgehung und 8 Ports (Ersatzteil)

PID	Beschreibung
CSF6K-XNM-8X10G	1/10-Gbit/s-SFP+-Netzwerkmodul mit 8 Ports
CSF6K-XNM-8X10G=	1/10-Gbit/s-SFP+-Netzwerkmodul mit 8 Ports (Ersatzteil)
CSF6K-XNM-8X25G	1/10/25-Gbit/s-ZSFP-Netzwerkmodul mit 8 Ports
CSF6K-XNM-8X25G=	1/10/25-Gbit/s-ZSFP-Netzwerkmodul mit 8 Ports (Ersatzteil)
CSF6K-XNM-4X40G	40-Gbit/s-QSFP+-Netzwerkmodul mit 4 Ports
CSF6K-XNM-4X40G=	40-Gbit/s-QSFP+-Netzwerkmodul mit 4 Ports
CSF6K-XNM-2X100G	100-Gbit/s-QSFP+-Netzwerkmodul mit 2 Ports
CSF6K-XNM-2X100G=	100-Gbit/s-QSFP+ mit 2 Ports (Ersatzteil)
CSF6K-XNM-4X200G	40/100/200-Gbit/s-QSFP+-Netzwerkmodul mit 4 Ports
CSF6K-XNM-4X200G=	40/100/200-Gbit/s-QSFP+-Netzwerkmodul mit 4 Ports (Ersatzteil)
CSF6K-XNM-2X400G	40/100/200/400-Gbit/s-QSFP-DD mit 2 Ports
CSF6K-XNM-2X400G=	40/100/200/400-Gbit/s-QSFP-DD mit 2 Ports (Ersatzteil)
CSF6100-NM-BLANK	Platzhalter für einen leeren Steckplatz eines Netzwerkmoduls
CSF6100-NM-BLANK=	Platzhalter für einen leeren Steckplatz eines Netzwerkmoduls (Ersatzteil)

Netzkabelspezifikationen

Jedes Netzteil verfügt über ein eigenes Netzkabel. Für den Anschluss an die Cisco Secure Firewall sind Standard-Netzkabel oder Jumper-Kabel verfügbar. Die Jumper-Kabel für den Einsatz in Racks sind als Alternative zu den Standard-Netzkabeln erhältlich.

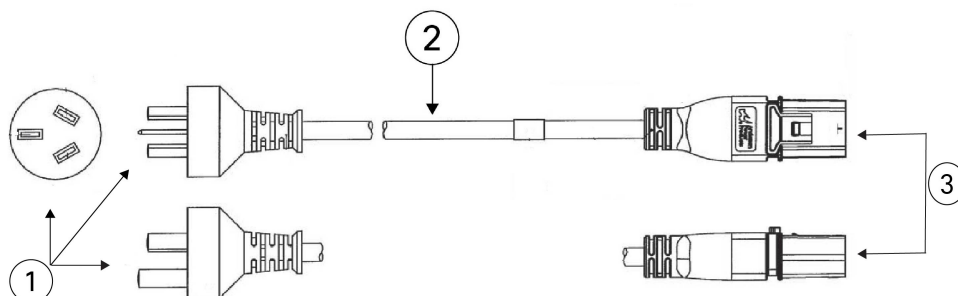
Wenn Sie das optionale Netzkabel nicht zusammen mit dem System bestellen, übernehmen Sie die Verantwortung für die Auswahl des richtigen Netzkabels für das Produkt. Die Verwendung eines nicht kompatiblen Netzkabels mit diesem Produkt kann zu elektrischen Sicherheitsrisiken führen. Bei Bestellungen, die nach Argentinien, Brasilien und Japan ausgeliefert werden, muss das jeweilige Netzkabel zusammen mit dem System bestellt werden.



Hinweis Es werden nur die zulässigen Netzkabel oder Jumper-Netzkabel unterstützt, die mit der Secure Firewall 6100-Serie ausgeliefert werden.

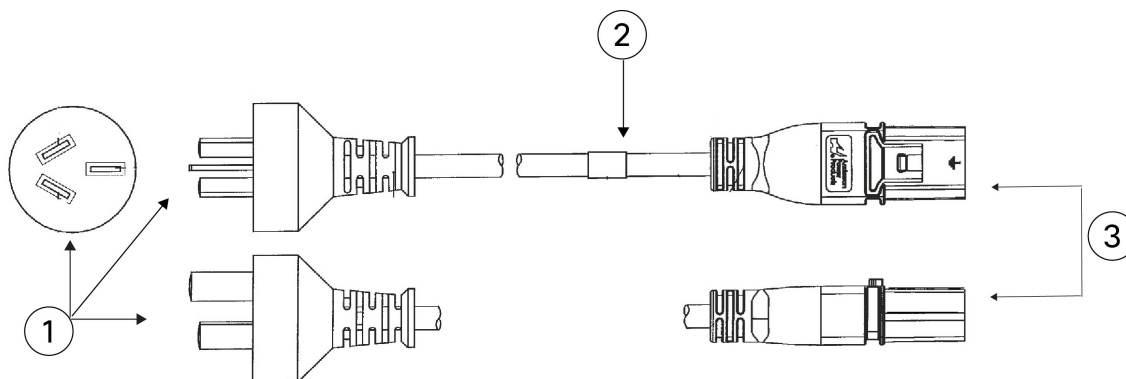
Die folgenden AC-Netzkabel werden unterstützt. Ein Ende des Kabels hat einen Steckverbinder vom Typ Anderson Saf-D-Grid.

Abbildung 20: Argentinien



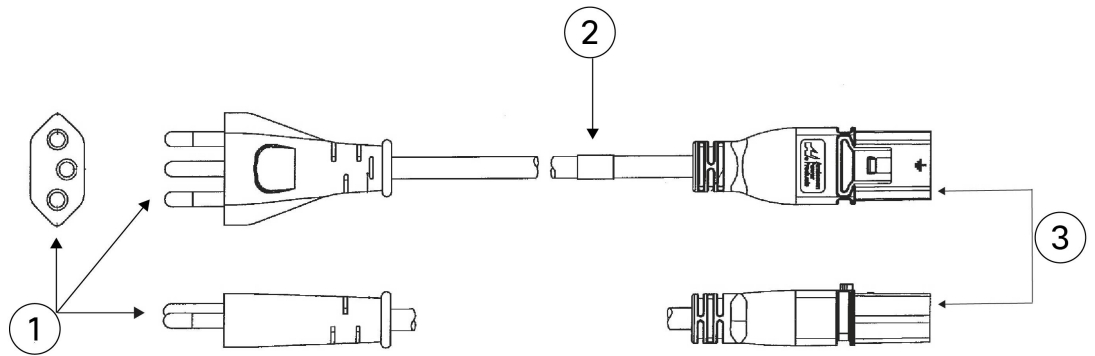
	PID: CAB-AC-16A-SG-AR	Teilenummer: 37-1649-01
1	Stecker: IRAM 2073	2 Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid	Kabellänge: 4,3 m

Abbildung 21: Australien/Neuseeland



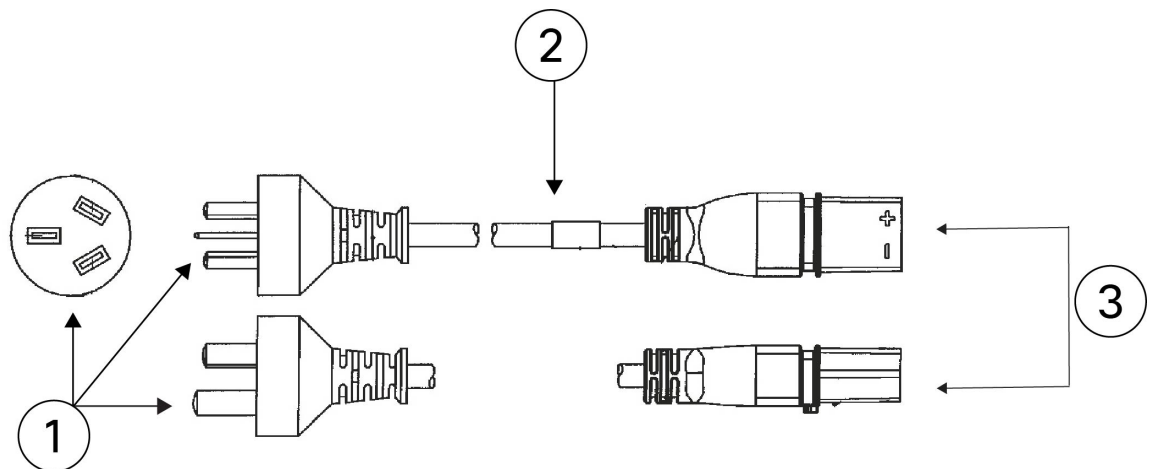
	PID: CAB-AC-16A-SG-AZ	Teilenummer: 37-1661-01
1	Stecker: AU20LS3	2 Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid	Kabellänge: 4,3 m

Abbildung 22: Brasilien



	PID: CAB-AC-16A-SG-BR		Teilenummer: 37-1650-01
1	Stecker: EL224	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

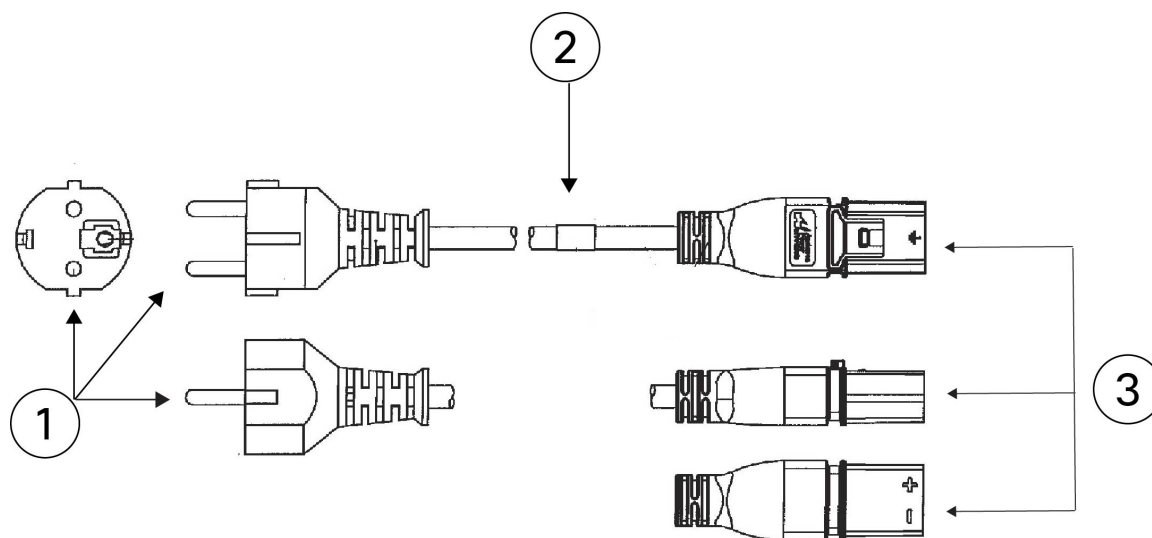
Abbildung 23: China



	PID: CAB-AC-16A-SG-CH		Teilenummer: 37-1655-01
1	Stecker: GB 16C	2	Kabelnennwerte: 16 A, 250 V

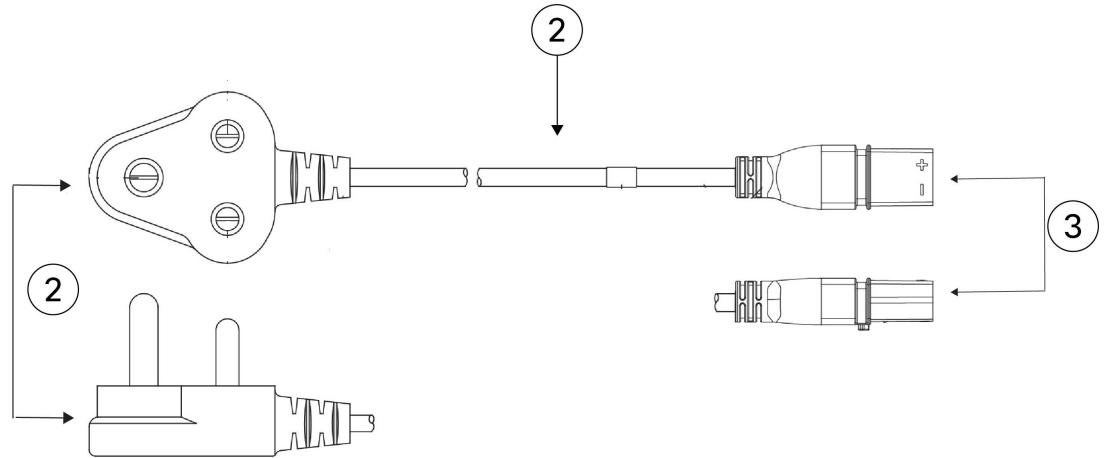
3 Anschluss: Saf-D-Grid	Kabellänge: 4,3 m
-------------------------	-------------------

Abbildung 24: Europa



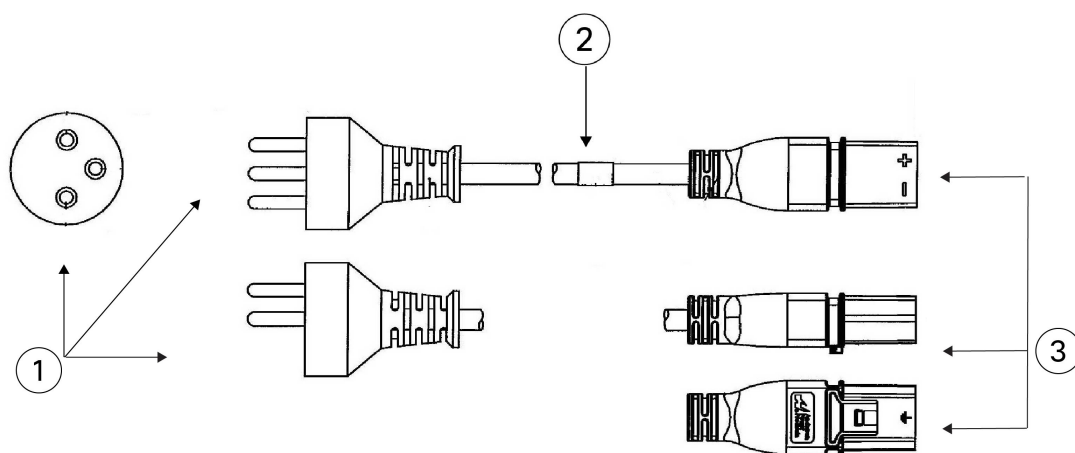
PID: CAB-AC-16A-SG-EU	Teilenummer: 37-1660-01
1 Stecker: CEE 7/7	2 Kabelnennwerte: 16 A, 250 V
3 Anschluss: Saf-D-Grid	Kabellänge: 4,3 m

Abbildung 25: Indien



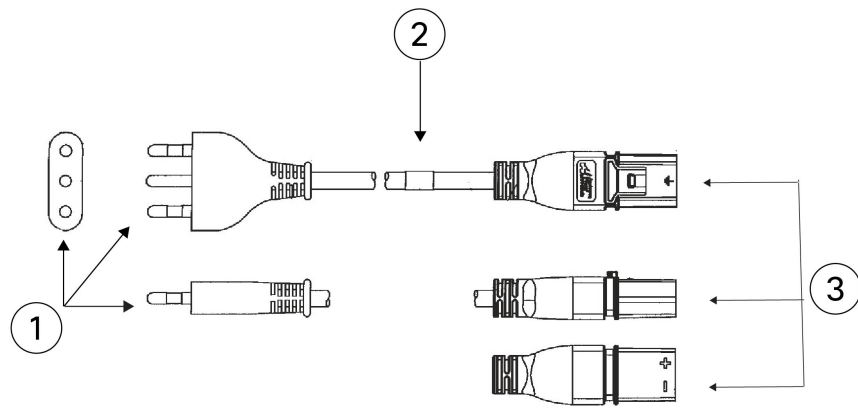
	PID: CAB-AC-16A-SG-IND		Teilenummer: 37-1863-01
1	Stecker: SABS 164-1	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 26: Israel



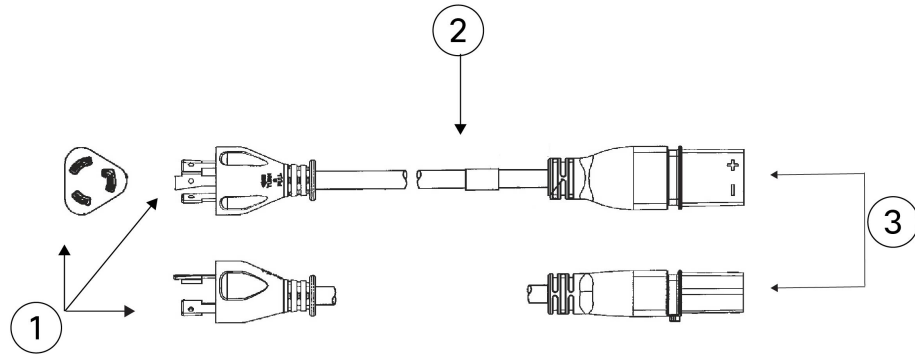
	PID: CAB-AC-16A-SG-IS		Teilenummer: 37-1658-01
1	Stecker: SI 16S3	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 27: Italien



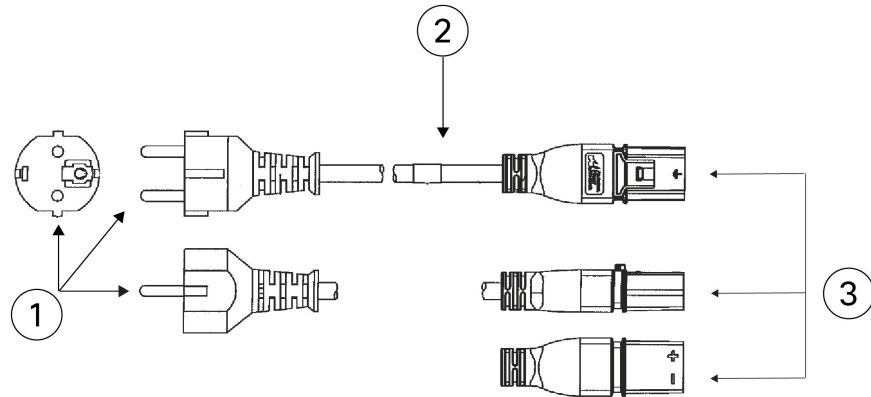
	PID: CAB-AC-16A-SG-IT		Teilenummer: 37-1651-01
1	Stecker: CEI 23-50	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 28: Japan



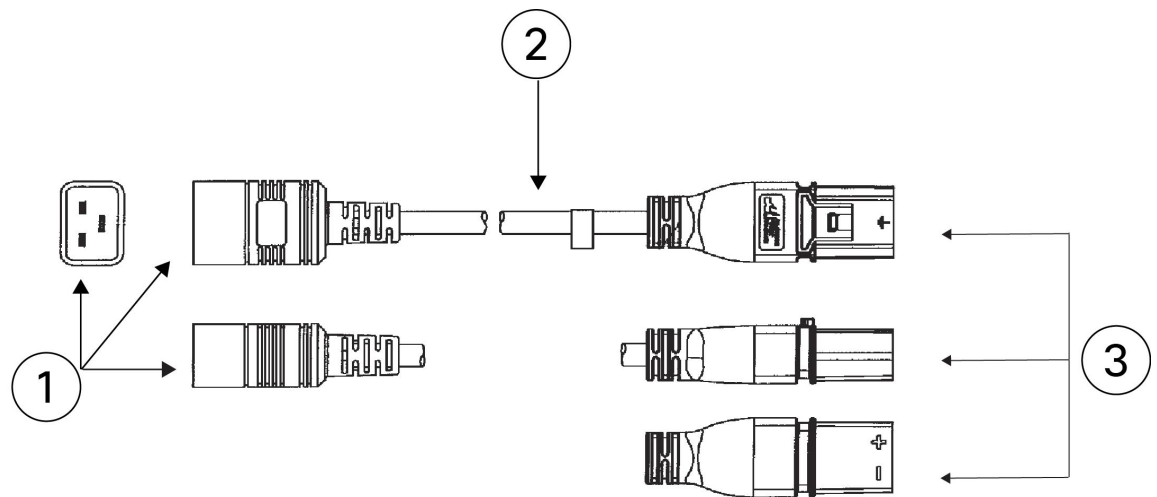
	PID: CAB-AC-16A-SG-JPN		Teilenummer: 37-1656-01
1	Stecker: NEMA L6-20	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 29: Korea



	PID: CAB-AC-16A-SG-SK		Teilenummer: 37-1646-01
1	Stecker: Src	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

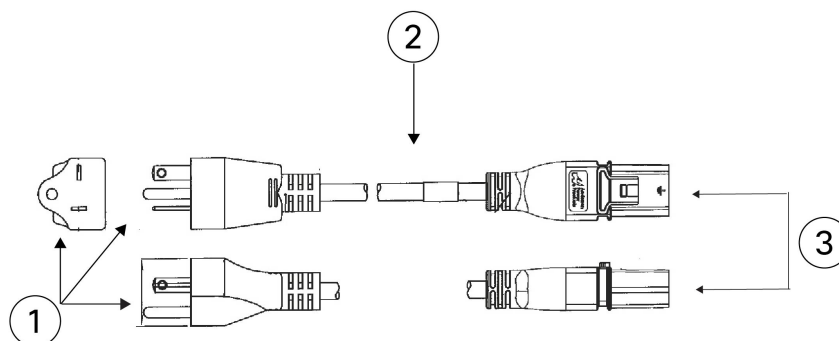
Abbildung 30: Nordamerika: Jumper-Schaltschrank-Leistungsverteilungseinheit (PDU)



	PID: CAB-AC-20A-SG-C20		Teilenummer: 37-1653-01
--	------------------------	--	-------------------------

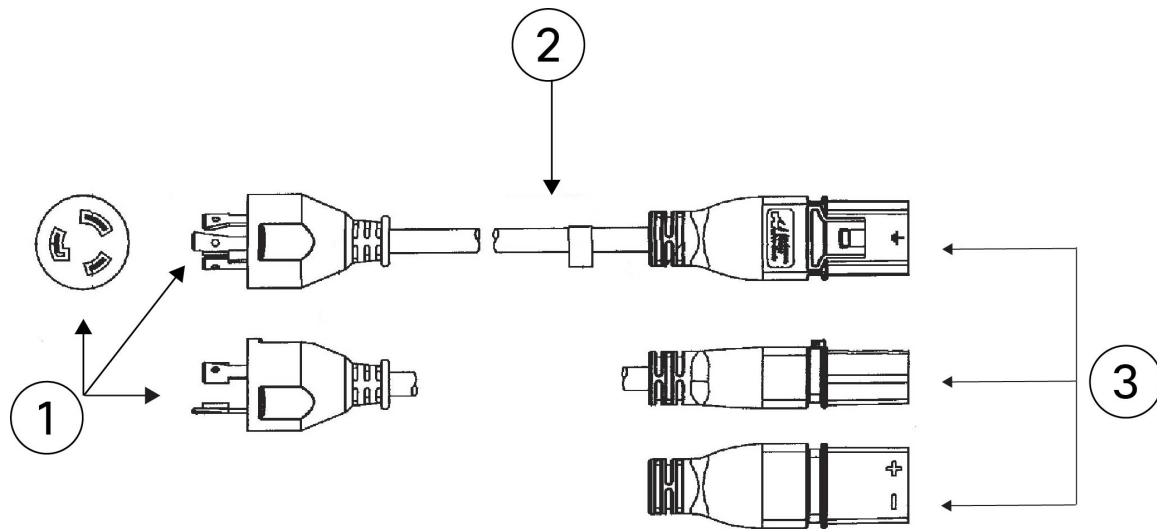
1	Stecker: IEC C20	2	Kabelnennwerte: 20 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 31: Nordamerika, Flachstecker 125 V



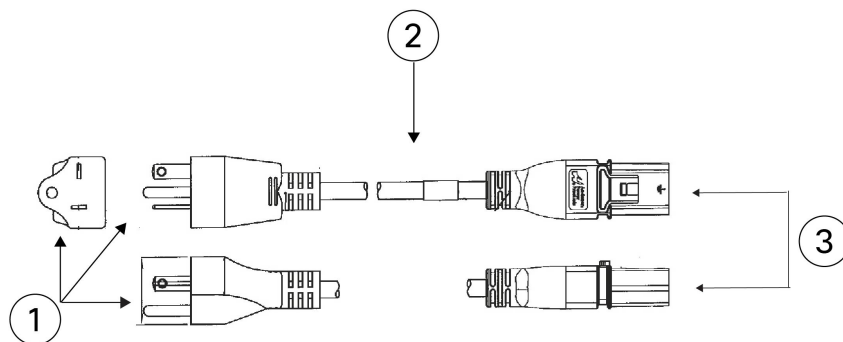
	PID: CAB-AC-20A-SG-US		Teilenummer: 37-1662-01
1	Stecker: NEMA 5-20P	2	Kabelnennwerte: 20 A, 125 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 32: Nordamerika, Twistlock 125 V



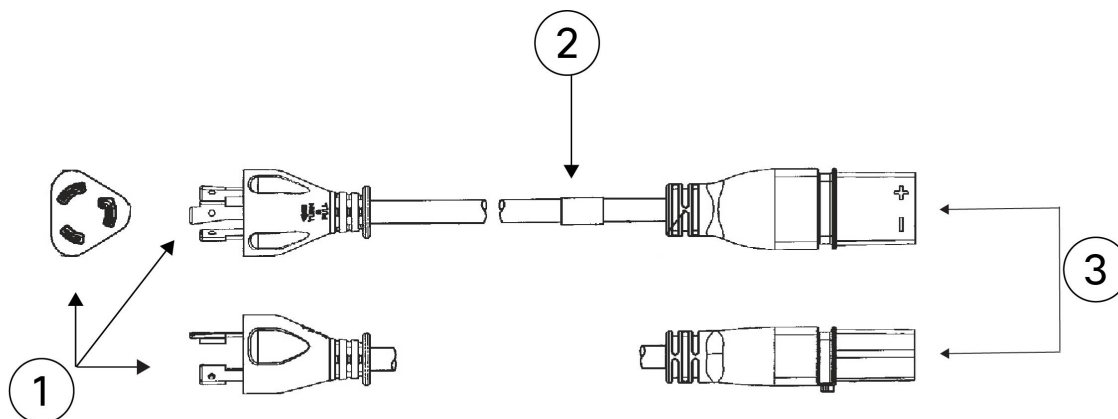
	PID: CAB-AC-20A-SG-US1		Teilenummer: 37-1652-01
1	Stecker: NEMA L5-20	2	Kabelnennwerte: 20 A, 125 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 33: Nordamerika, Flachstecker 250 V



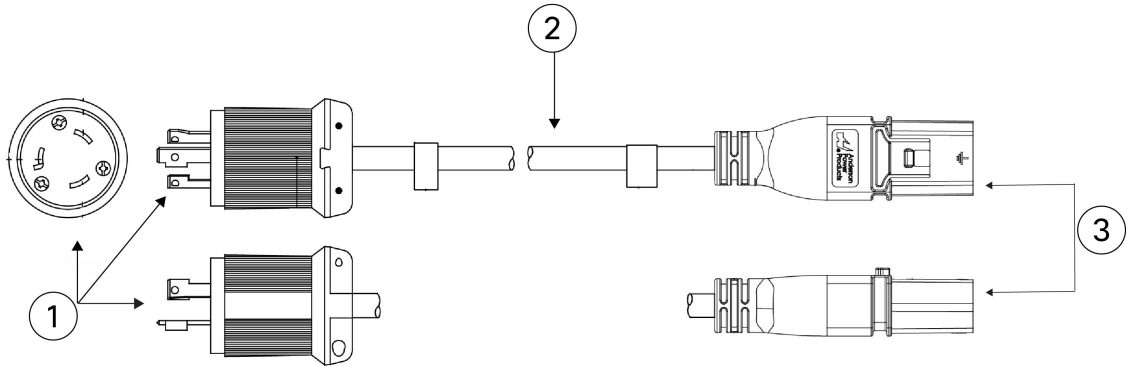
	PID: CAB-AC-20A-SG-US2		Teilenummer: 37-1657-01
1	Stecker: NEMA 6-20	2	Kabelnennwerte: 20 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 34: Nordamerika, Twist Lock 250 V



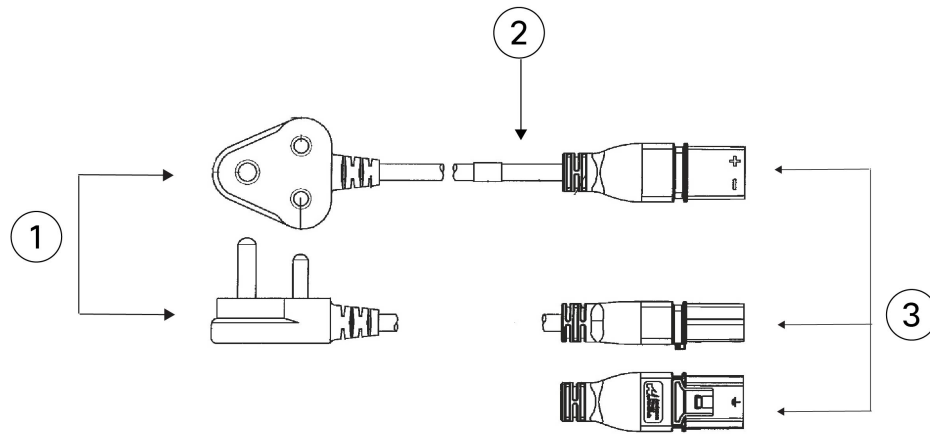
	PID: CAB-AC-20A-SG-US3		Teilenummer: 37-1656-01
1	Stecker: NEMA L6-20	2	Kabelnennwerte: 20 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 35: Nordamerika, Twist Lock 277 V



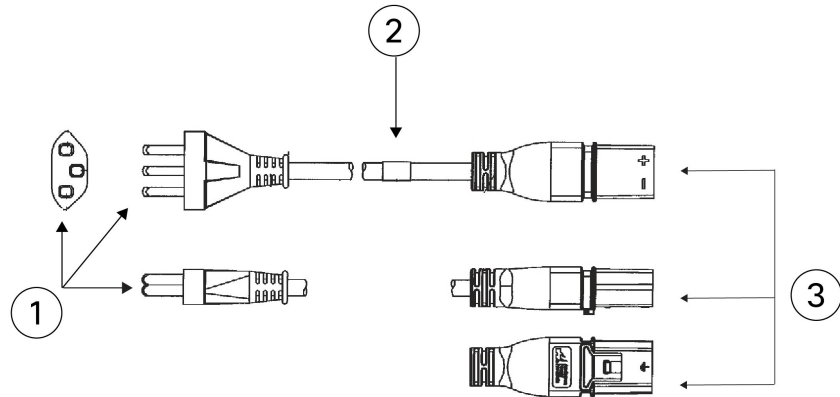
	PID: CAB-AC-20A-SG-US4		Teilenummer: 37-1645-01
1	Stecker: NEMA L7-20P	2	Kabelnennwerte: 20 A, 277 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 36: Südafrika



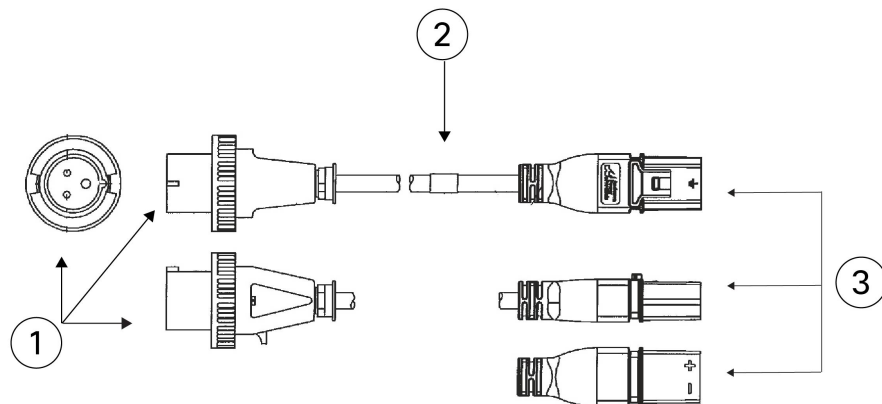
	PID: CAB-AC-16A-SG-SA		Teilenummer: 37-1647-01
1	Stecker: EL	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 37: Schweiz



	PID: CAB-AC-16A-SG-SW		Teilenummer: 72-1654-01
1	Stecker: SEV 5934-2	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Abbildung 38: Vereinigtes Königreich



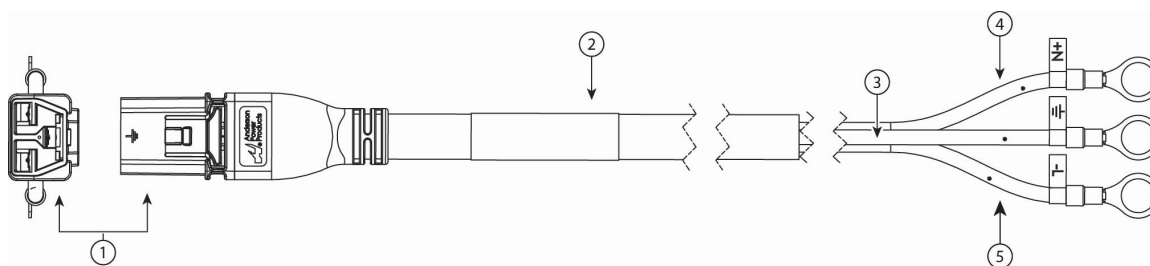
	PID: CAB-AC-16A-SG-IN		Teilenummer: 37-1659-01
1	Stecker: IEC 60309	2	Kabelnennwerte: 16 A, 250 V
3	Anschluss: Saf-D-Grid		Kabellänge: 4,3 m

Die folgenden HVDC-Netzkabel werden unterstützt. Ein Ende des Kabels hat einen Steckverbinder vom Typ Anderson Saf-D-Grid, am andere Ende weist es drei Pigtail-Drähten auf. Die Größe des Spiralkabelbolzens für den isolierten Ringkabelschuh beträgt für die folgenden Kabel 9,5 mm (3/8 Zoll).



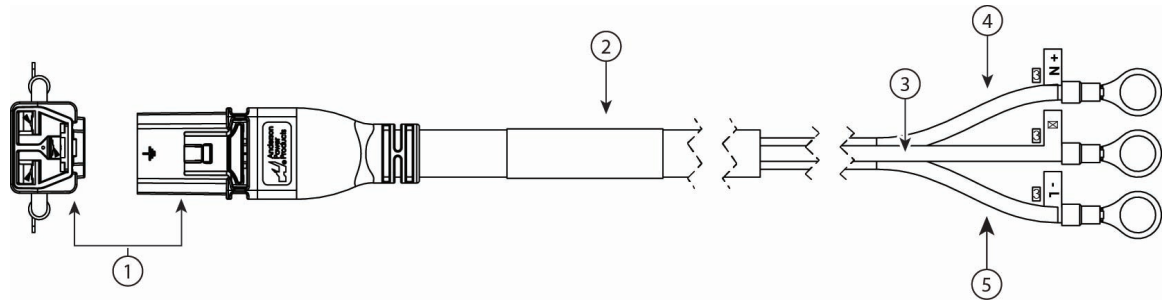
Hinweis Zur empfohlenen 6AWG-Kupferdrahtstärke passende Gleichstromkabel müssen Sie selbst bereitstellen. Die Laschen sind bereits im Lieferumfang der DC-Netzteile für die Cisco Firewall 6100 enthalten.

Abbildung 39: HVDC, Nordamerika



	PID: CAB-HVDC-2M		Teilenummer: 72-100766-01
1	Anschluss: Saf-D-Grid	2	Kabelnennwert: 18 A, 400 VDC
3	Grüner Draht	4	Weißer Draht
5	Schwarzer Draht		Kabellänge: 2,0 m

Abbildung 40: HVDC, international und China CCC-konform



	PID: CAB-HVDC-3T-2M		Teilenummer: 72-100812-01
1	Anschluss: Saf-D-Grid	2	Kabelnennwert: 25 A, 400 VDC
3	Grün-gelber Draht	4	Blauer Draht
5	Brauner Draht		Kabellänge: 2,0 m



KAPITEL 2

Vorbereitung der Installation

- [Warnhinweise für die Installation, auf Seite 71](#)
- [Sicherheitshinweise, auf Seite 73](#)
- [Sicherheit bei Arbeiten mit Elektrizität, auf Seite 74](#)
- [Vermeidung von Schäden durch ESD, auf Seite 74](#)
- [Standortumgebung, auf Seite 75](#)
- [Standortbezogene Überlegungen, auf Seite 75](#)
- [Überlegungen zur Stromversorgung, auf Seite 75](#)
- [Überlegungen zur Rack-Konfiguration, auf Seite 76](#)

Warnhinweise für die Installation

Lesen Sie vor der Installation der Sicherheits-Appliance das Dokument mit den [Erfüllung gesetzlicher Auflagen und Sicherheitsinformationen](#).

Beachten Sie die folgenden Warnhinweise:



Warnung **Anweisung 1071** – Definition der Warnhinweise

WICHTIGE SICHERHEITSANWEISUNGEN

Bevor Sie an Geräten arbeiten, sollten Sie sich über die mit elektrischen Schaltkreisen verbundenen Gefahren bewusst und mit den Standardverfahren zur Unfallverhütung vertraut sein. Lesen Sie die Installationshinweise, bevor Sie das System nutzen, installieren oder an die Stromversorgung anschließen. Suchen Sie mit der am Anfang jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen für dieses Gerät.

BEWAHREN SIE DIESE ANWEISUNGEN SICHER AUF.





Warnung **Anweisung 1005** – Leitungsschutzschalter

Dieses Produkt ist für Gebäude mit Kurzschlussicherung (Überstromschutz) gedacht. Stellen Sie sicher, dass der Nennwert der Schutzvorrichtung folgenden Wert nicht überschreitet:

AC/HVAC/HVDC = 20 A (Nordamerika)

AC/HVAC/HVDC = 16 A (international)



Warnung **Anweisung 1017** – Bereiche mit beschränktem Zutritt

Dieses Gerät ist zur Installation in Bereichen mit beschränktem Zutritt vorgesehen. Bereiche mit beschränktem Zutritt dürfen nur von geschulten und qualifizierten Personen betreten werden.



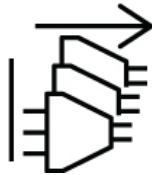
Warnung **Anweisung 1024** – Erdungsleiter

Dieses Gerät muss geerdet sein. Auf keinen Fall den Erdungsleiter unwirksam machen oder das Gerät ohne einen sachgerecht installierten Erdungsleiter verwenden, um die Stromschlag- und Brandgefahr zu minimieren. Wenn Sie sich nicht sicher sind, ob eine sachgerechte Erdung vorhanden ist, wenden Sie sich an die zuständige Inspektionsbehörde oder einen Elektriker.



Warnung **Anweisung 1028** – Mehr als eine Netzteil

Dieses Gerät kann mit mehr als einem Netzteil verbunden sein. Um die Stromschlag- und Brandgefahr zu minimieren und um sicherzustellen, dass die Stromversorgung der Einheit abgeschaltet ist, müssen alle Anschlüsse entfernt werden.



Warnung **Anweisung 1029** – Leere Frontplatten und Abdeckungen

Leere Frontplatten und Abdeckungen dienen drei wichtigen Funktionen: Sie minimieren die Stromschlag- und Brandgefahr, sie schirmen elektromagnetische Interferenzen (EMI) ab, die möglicherweise andere Geräte stören, und sie leiten Kühlluft durch das Chassis. Betreiben Sie das System nur, wenn alle Karten, Frontplatten, Frontabdeckungen und hinteren Abdeckungen installiert sind.

**Warnung** **Anweisung 1051** – Laserstrahlung

Von getrennten Fasern oder Anschlüssen kann unsichtbare Laserstrahlung ausgehen. Blicken Sie nicht direkt in Strahlen oder optische Instrumente.

**Warnung** **Anweisung 1055** – Laser der Klasse 1/1M

Unsichtbare Laserstrahlung ist vorhanden. Setzen Sie BenutzerInnen von Teleskopoptiken keinem Risiko aus. Dies gilt für Laserprodukte der Klasse 1/1M.

**Warnung** **Anweisung 1074** – Übereinstimmung mit örtlichen und nationalen elektrischen Richtlinien und Bestimmungen

Die Installation des Geräts muss in Übereinstimmung mit den örtlichen und nationalen elektrischen Richtlinien und Bestimmungen erfolgen, um die Stromschlag- und Brandgefahr zu minimieren.

**Hinweis** **Anweisung 1089** – Definitionen: geschulte und qualifizierte Person

Als geschulte Person wird eine Person definiert, die von einer qualifizierten Person ausgebildet und geschult wurde. Sie unternimmt die nötigen Vorsichtsmaßnahmen bei der Arbeit mit den Geräten.

Eine qualifizierte Person/qualifiziertes Fachpersonal ist eine Person, die geschult wurde oder über Erfahrung mit den Geräten verfügt und potenzielle Gefahren bei der Arbeit mit den Geräten kennt.

**Warnung** **Anweisung 1091** – Installation durch eine geschulte Person

Das Installieren, Ersetzen oder Warten dieses Geräts sollte ausschließlich einer geschulten oder qualifizierten Person gestattet werden. Siehe Anweisung 1089 für eine Definition von geschulten oder qualifizierten Personen.

Sicherheitshinweise

Beachten Sie die folgenden Sicherheitsrichtlinien:

- Halten Sie den Bereich vor, während und nach der Installation sauber und staubfrei.
- Legen Sie Ihre Werkzeuge nicht in Gangflächen ab, wo Sie oder andere darüber stolpern könnten.
- Tragen Sie keine losen Kleidungsstücke oder Schmuck, wie Ohringe, Armbänder oder Halsketten, die sich im Chassis verfangen könnten.
- Tragen Sie bei Arbeiten unter Bedingungen, die möglicherweise die Augen gefährden, eine Schutzbrille.

- Unterlassen Sie alles, was eine Gefahr für Personen darstellen kann oder die Sicherheit des Geräts beeinträchtigt.
- Versuchen Sie niemals, ein Objekt anzuheben, das für eine Person allein zu schwer ist.

Sicherheit bei Arbeiten mit Elektrizität



Warnung Bevor Sie an einem Chassis arbeiten, stellen Sie sicher, dass das Netzkabel abgezogen ist.

Lesen Sie vor der Installation des Chassis das Dokument [Gesetzliche Auflagen und Sicherheitshinweise](#).

Befolgen Sie bei Arbeiten an mit elektrischem Strom betriebenen Geräten diese Richtlinien:

- Bevor Sie mit einem Verfahren beginnen, bei dem Sie auf das Innere des Chassis zugreifen müssen, lokalisieren Sie den Notaus-Schalter in dem Raum, in dem Sie arbeiten. Wenn es zu einem elektrischen Unfall kommt, schalten Sie die Stromzufuhr so schnell wie möglich aus.
- Arbeiten Sie nicht allein, wenn an Ihrem Arbeitsplatz potenziell gefährliche Bedingungen vorhanden sind.
- Nehmen Sie niemals an, dass die Stromversorgung getrennt ist. Überprüfen Sie dies stets.
- Suchen Sie sorgfältig nach möglichen Gefahren in Ihrem Arbeitsbereich, z. B. feuchten Böden, nicht geerdeten Verlängerungskabeln, durchgeschauerten Netzkabeln und fehlenden Schutzerdungen.
- Bei einem elektrischen Unfall:
 - Seien Sie vorsichtig, und werden Sie nicht selbst zum Opfer.
 - Trennen Sie die Stromversorgung des Systems.
 - Wenn möglich, bitten Sie eine andere Person, den Rettungsdienst zu rufen. Versuchen Sie andernfalls, den Zustand des Opfers einzuschätzen, und holen Sie dann Hilfe.
 - Bestimmen Sie, ob die Person Mund-zu-Mund-Beatmung oder eine Herzmassage benötigt; ergreifen Sie dann die geeigneten Maßnahmen.
- Verwenden Sie das Chassis mit der angegebenen Spannung und wie im Benutzerhandbuch angegeben.
- Das Chassis ist mit einem AC-Eingangsteil ausgestattet, das mit einem dreiadrigen Stromkabel mit Erdungsklemme versendet wird, die nur auf eine geerdete Steckdose passt. Versuchen Sie nicht, diese Sicherheitsfunktion zu umgehen. Die Erdung des Geräts muss den lokalen und nationalen elektrotechnischen Vorschriften entsprechen.

Vermeidung von Schäden durch ESD

ESD tritt auf, wenn elektronische Komponenten nicht ordnungsgemäß genutzt werden. Dadurch können Geräte und elektrische Schaltkreise beschädigt werden und einen temporären oder vollständigen Ausfall Ihrer Geräte verursachen.

Beachten Sie immer die Vorgehensweisen zur Vermeidung von Schäden durch elektrostatische Entladung, wenn Sie Komponenten ausbauen und ersetzen. Stellen Sie sicher, dass das Chassis geerdet ist. Verwenden Sie immer ein antistatisches Armband und stellen Sie guten Hautkontakt sicher. Verbinden Sie die Erdungsklemme mit einer unlackierten Fläche am Chassis-Rahmen, um ESD-Spannungen sicher zu erden. Zum zuverlässigen Schutz vor Beschädigungen durch ESD und vor Stromschlägen müssen das Armband und der Leiter wirksam funktionieren. Wenn kein Armband verfügbar ist, erden Sie sich durch Berühren des Metallteils am Chassis.

Überprüfen Sie zu Ihrem Schutz regelmäßig den Widerstandswert des antistatischen Armbands. Er sollte zwischen einem und 10 Megohm liegen.

Standortumgebung

Unter [Hardwarespezifikationen, auf Seite 49](#) finden Sie Informationen zu den physischen Spezifikationen.

Planen Sie das Layout des Standorts und die Positionen der Geräte sorgfältig, um Geräteausfälle zu vermeiden und die Wahrscheinlichkeit umgebungsbedingter Systemabschaltungen zu verringern. Sollte es bei Ihren derzeitigen Geräten zu Systemabschaltungen oder ungewöhnlich hohen Fehlerraten kommen, können Sie mithilfe dieser Empfehlungen die Ursache der Ausfälle lokalisieren und künftige Probleme vermeiden.

Standortbezogene Überlegungen

Berücksichtigen Sie die folgenden Punkte, um eine angemessene Betriebsumgebung für das Chassis zu planen und umgebungsbedingte Geräteausfälle zu vermeiden.

- Elektrische Geräte erzeugen Wärme. Die Umgebungstemperatur reicht möglicherweise nicht aus, um die Geräte ohne angemessene Luftzirkulation auf die erforderliche Betriebstemperatur herunterzukühlen. Stellen Sie sicher, dass der Raum, in dem Sie Ihr System ausführen, über eine ausreichende Luftzirkulation verfügt.
- Stellen Sie sicher, dass die Chassis-Abdeckung sicher verschlossen ist. Das Chassis ist so konzipiert, dass Kaltluft darin effektiv zirkulieren kann. Ein offenes Chassis führt zu undichten Stellen, wodurch der Kaltluftstrom an den internen Komponenten unterbrochen oder verringert werden kann.
- Beachten Sie immer die Vorgehensweisen zur Vermeidung von Schäden durch elektrostatische Entladung, um eine Beschädigung der Geräte zu vermeiden. Schäden durch elektrostatische Entladung können zu einem sofortigen oder temporären Geräteausfall führen.

Überlegungen zur Stromversorgung

Unter [Netzstrommodule, auf Seite 29](#) finden Sie detailliertere Informationen zur Stromversorgung im Chassis.

Beachten Sie bei der Installation des Chassis Folgendes:

- Vergewissern Sie sich vor der Installation des Chassis, dass die Stromversorgung am Standort frei von Spitzen und Störungen ist. Installieren Sie bei Bedarf ein Netzschutzgerät, um ein angemessenes Spannungs- und Stromniveau in der Eingangsspannung der Appliance sicherzustellen.
- Installieren Sie eine geeignete Erdung für den Standort, um Schäden durch Blitzschlag und Stromanstiege zu vermeiden.

- Der Betriebsbereich des Chassis kann nicht durch den User festgelegt werden. Entnehmen Sie die korrekten Eingangsstromanforderungen der Appliance dem Etikett auf dem Chassis.
- Es stehen verschiedene Arten von AC-Netzkabeln für das Chassis zur Verfügung. Vergewissern Sie sich, dass Sie das korrekte Kabel für Ihren Standort erhalten haben.
- Falls Sie doppelte redundante (1+1) Netzteile verwenden, empfehlen wir Ihnen die Nutzung unabhängiger Stromkreise für jedes der Netzteile.
- Installieren Sie, falls möglich, eine unterbrechungsfreie Stromversorgung für Ihren Standort.

Überlegungen zur Rack-Konfiguration

Unter [Rackmontage des Chassis mit Gleitschienen, auf Seite 78](#) finden Sie die Vorgehensweise zur Rackmontage des Chassis.

Beachten Sie beim Planen der Rack-Konfiguration die folgenden Punkte:

- Standardmäßiges 19-Zoll-EIA-Rack (48,3 cm) mit 4 Säulen und Montageschienen, die dem universellen Bohrungsabstand gemäß Abschnitt 1 von ANSI/EIA-310-D-1992 entsprechen.
- Die Rackmontagesäulen müssen 2 bis 3,5 mm dick sein, damit die Rack-Montage an Gleitschienen möglich ist.
- Wenn Sie ein Chassis in einem offenen Rack montieren, stellen Sie sicher, dass der Rack-Rahmen die Ein- und Auslassöffnungen nicht blockiert.
- Wenn Ihr Rack Türen an der Vorder- oder Rückseite hat, müssen 65 % der Fläche gleichmäßig von oben nach unten perforiert sein, um für eine ausreichende Luftzirkulation zu sorgen.
- Stellen Sie sicher, dass geschlossene Racks ausreichend belüftet werden. Stellen Sie sicher, dass das Rack nicht zu voll ist, da jedes Chassis Wärme erzeugt. Ein geschlossenes Rack sollte seitliche Luftschlitze und einen Lüfter haben, um Kühlluft zur Verfügung zu stellen.
- In einem geschlossenen Rack mit einem Lüfter oben kann die von Geräten im unteren Bereich des Racks erzeugte Wärme in die Einlassöffnungen der darüberliegenden Einheiten gezogen werden. Stellen Sie sicher, dass Einheiten im unteren Bereich des Racks ausreichend belüftet werden.
- Leitbleche können dazu beitragen, Abluft von der Ansaugluft zu trennen, was auch die Kühlluftzirkulation durch das Chassis verbessert. Die beste Platzierung der Leitbleche hängt von den Luftstrommustern im Rack ab. Probieren Sie verschiedene Varianten aus, um die beste Position für die Leitbleche zu finden.



KAPITEL 3

Montage des Chassis

- [Auspacken und Prüfen des Chassis, auf Seite 77](#)
- [Rackmontage des Chassis mit Gleitschienen, auf Seite 78](#)
- [Erdung des Chassis, auf Seite 85](#)

Auspacken und Prüfen des Chassis



Hinweis Das Chassis wird vor dem Versand gründlich geprüft. Wenn während des Transports ein Schaden aufgetreten ist oder Artikel fehlen, wenden Sie sich umgehend an Ihren Kundenservicemitarbeiter. Bewahren Sie den Versandbehälter auf, falls Sie das Chassis aufgrund von Beschädigungen zurücksenden müssen.

Unter [Lieferumfang, auf Seite 4](#) finden Sie eine Liste der Artikel, die im Lieferumfang des Chassis enthalten sind.

Prozedur

-
- Schritt 1** Nehmen Sie das Chassis aus dem Karton und bewahren Sie das gesamte Verpackungsmaterial auf.
- Schritt 2** Vergleichen Sie die Lieferung mit der Geräteliste, die Sie von Ihrem zuständigen Kundendienstmitarbeiter erhalten haben. Prüfen Sie, ob Sie alle Teile erhalten haben.
- Schritt 3** Überprüfen Sie die Lieferung auf Schäden und melden Sie etwaige Unstimmigkeiten oder Schäden bei Ihrem Kundenservicemitarbeiter. Halten Sie hierzu bitte folgende Informationen bereit:
- Rechnungsnummer des Versenders (siehe Lieferschein)
 - Modell- und Seriennummer des beschädigten Geräts
 - Beschreibung des Schadens
 - Auswirkungen von Schäden auf die Installation
-

Rackmontage des Chassis mit Gleitschienen

Dieses Verfahren beschreibt den Einbau der Secure Firewall 6100 in ein Rack mithilfe von Gleitschienen. Es gilt für alle Modelle der Secure Firewall 6100-Serie. Sie verwenden die Stifte am Chassis, um die Gleitschiene zu sichern. Eine Liste der PIDs im Zusammenhang mit dem Rack-Einbau des Chassis finden Sie im Abschnitt [Produkt-IDs, auf Seite 50](#). Sie können die optionale Kabelmanagement-Halteklammer bei allen Modellen der Cisco Secure Firewall 6100 installieren.

Bei dem Rack handelt es sich um ein EIA-Standardrack (Electronic Industries Association). Es handelt sich um eine 4-Post-EIA-310-D, das ist die aktuelle Revision gemäß EIA. Der vertikale Bohrungsabstand wechselt zwischen 12,70 mm (0,50 Zoll) und 15,90 mm (0,625 Zoll) und wiederholt sich. Der Start- und Stoppbereich befindet sich in der Mitte der 12,70 mm-Bohrungen (0,50 Zoll). Der horizontale Abstand beträgt 465,1 mm (18,312 Zoll), und die Rack-Öffnung ist auf mindestens 450 mm (17,75 Zoll) festgelegt.

Die Gleitschienen sind mit Racks mit vier Säulen und Schränken mit quadratischen Steckplätzen, runden 7,1-mm-Löchern, #10-32-Gewindelöchern und #12-24-Gewindelöchern auf der Vorderseite der Rack-Säulen kompatibel. Die Gleitschiene ist mit Abständen der Rack-Säulen von vorne nach hinten zwischen 61–91 mm kompatibel. Die Rackmontagesäulen müssen 2 bis 3,5 mm dick sein, damit die Rack-Montage an Gleitschienen möglich ist.

Installationsvoraussetzungen für die Gleitschiene

Folgendes wird benötigt, um die Secure Firewall 6100 mit Gleitschienen in einem Rack zu installieren:

- Kreuzschlitzschraubendreher
- Zwei Gleitschienen
- Gleitschienen-Zubehör-Kit:
 - Zwei Gleitschienen-Montageklammern
 - Sechs Kreuzschlitzschrauben (8–32 x 0,302-Zoll) für die Gleitschienen-Montageklammern zur Befestigung der Halterungen am Chassis
 - Zwei Kreuzschlitzschrauben (M3 x 0,5 x 6 mm) zur Befestigung des Chassis an Ihrem Rack
- Kabelmanagement-Halteklammer-Kit (optional)
 - Zwei Kabelmanagement-Halteklammern
 - Vier Kreuzschlitzschrauben (8–32 x 0,375-Zoll)

Sicherheitswarnungen

Beachten Sie die folgenden Warnhinweise:



Warnung **Anweisung 1006** – Warnhinweis zum Chassis bei der Rackmontage und -wartung

Treffen Sie bei der Montage oder Wartung des Geräts in einem Rack entsprechende Vorkehrungen, um Verletzungen durch eine mögliche Instabilität des Systems zu vermeiden. Beachten Sie zu Ihrer eigenen Sicherheit die folgenden Hinweise:

- Ist das Gerät das einzige im Rack, montieren Sie es unten im Rack.
 - Soll das Gerät in einem bereits teilweise gefüllten Rack montiert werden, bestücken Sie das Rack von unten nach oben, wobei die schwerste Komponente unten im Rack montiert wird.
 - Verfügt das Rack über Stabilisierungsvorrichtungen, installieren Sie zunächst diese Vorrichtungen, bevor Sie ein Gerät im Rack montieren oder warten.
-



Warnung **Anweisung 1024** – Erdungsleiter

Dieses Gerät muss geerdet sein. Auf keinen Fall den Erdungsleiter unwirksam machen oder das Gerät ohne einen sachgerecht installierten Erdungsleiter verwenden, um die Stromschlag- und Brandgefahr zu minimieren. Wenn Sie sich nicht sicher sind, ob eine sachgerechte Erdung vorhanden ist, wenden Sie sich an die zuständige Inspektionsbehörde oder einen Elektriker.



Warnung **Anweisung 1098** — Anforderung zum Anheben

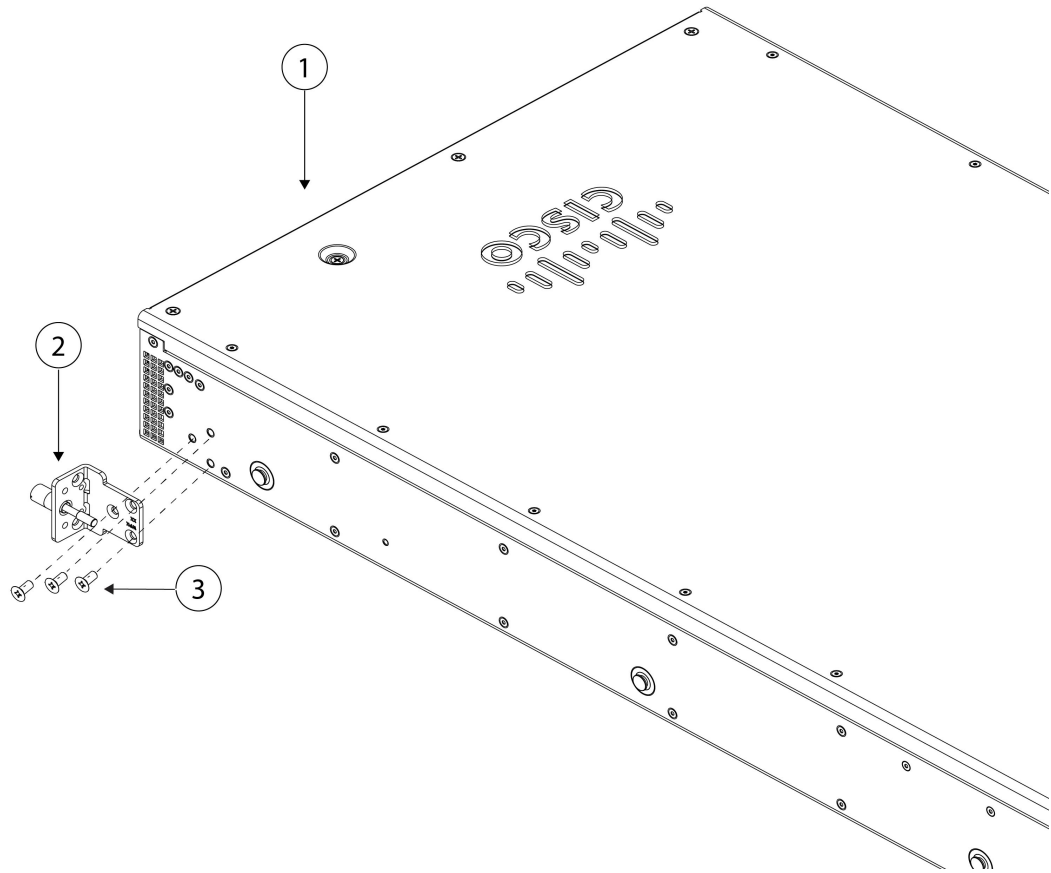
Zum Anheben der schweren Teile des Produkts sind zwei Personen erforderlich. Halten Sie Ihren Rücken gerade und heben Sie aus den Beinen und nicht aus dem Rücken, um Verletzungen zu vermeiden.

Prozedur

Schritt 1

Befestigen Sie die Gleitschienen-Verriegelungsbügel an jeder Seite des Chassis mit den sechs 8–32 x 0,302-Zoll-Kreuzschlitzschrauben (drei pro Seite).

Abbildung 41: Befestigen der Gleitschienen-Verriegelungsbügel



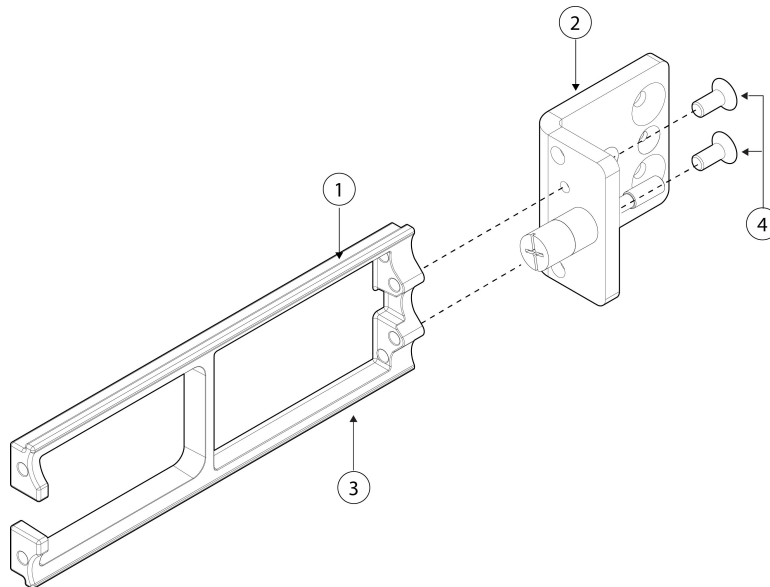
1	Vorderseite des Chassis	2	Gleitschienen-Verriegelungsbügel
3	8-32 x 0,302-Zoll-Kreuzschlitzschrauben (drei pro Seite)		—

Schritt 2

(Optional) Anbringen der Kabelmanagement-Halteklammer am Gleitschienen-Verriegelungsbügel:

- a) Bringen Sie die Schrauben für das Kabelmanagement am Gleitschienen-Verriegelungsbügel an.

Abbildung 42: Anbringen der Schrauben für das Kabelmanagement am Gleitschienen-Verriegelungsbügel



1	Stufenkerbe an der Innenseite der Kabelmanagement-Halteklammer	2	Gleitschienen-Verriegelungsbügel
3	Kabelmanagement-Halteklammer		8-32 x 0,375-Zoll-Kreuzschlitzschrauben (zwei pro Halterung)

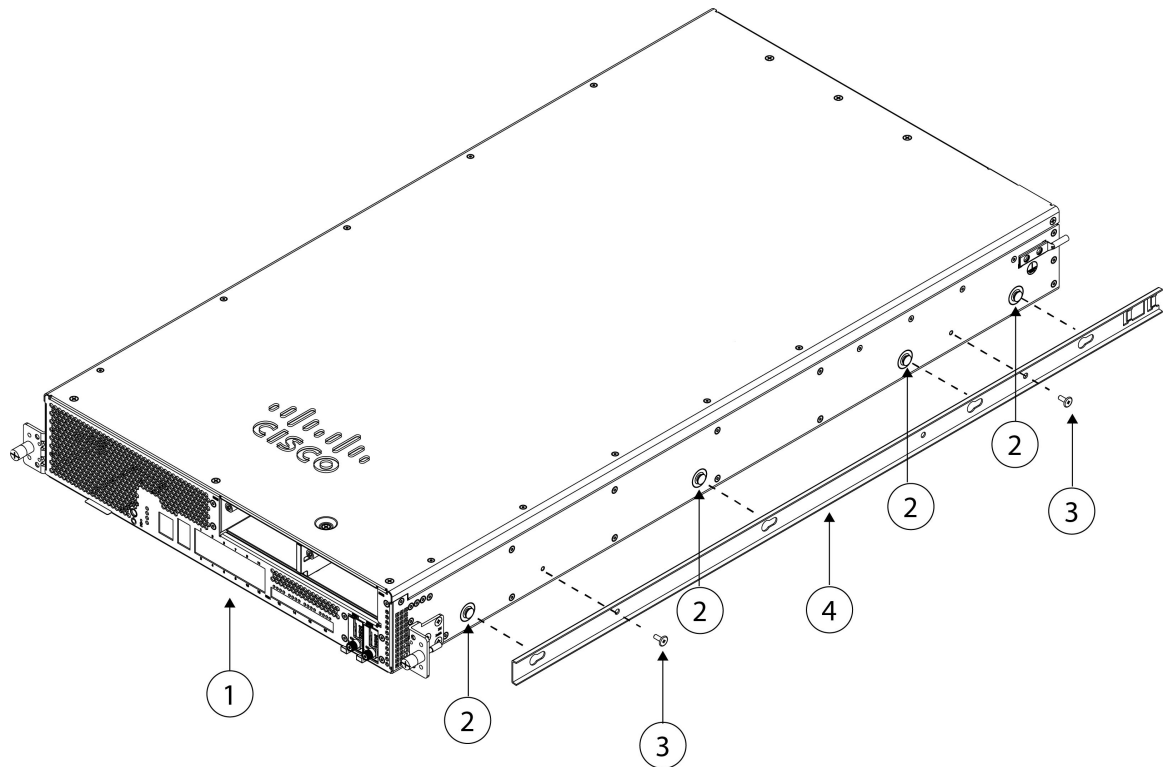
- b) Bringen Sie zwei 8-32 x 0,375-Zoll-Kreuzschlitzschrauben über die Innenseite des Gleitschienen-Verriegelungsbügels an, um die Kabelmanagement-Halteklammer an diesem zu sichern.

Schritt 3

Befestigen Sie die Innenschienen an den Seiten des Chassis:

- a) Entfernen Sie die Innenschienen von den Gleitschienen.
- b) Richten Sie eine Innenschiene an jeder Seite des Chassis aus. Richten Sie die Innenschiene so aus, dass die vier Schlitze an der Schiene mit den vier Stiften an der Seite des Chassis bündig sind.

Abbildung 43: Ausrichten der Innenschiene an den Stiften auf dem Chassis



1	Vorderseite des Chassis	2	Montagestift am Chassis für die Keilnut (vier pro Seite)
3	M3 x 0,5 x 6-mm-Kreuzschlitzschrauben (zwei pro Seite)	4	Innenschiene

- c) Bringen Sie die Keilnuten über den Schrauben/Stiften an und schieben Sie anschließend die Schiene zur Vorderseite, um sie an den Schrauben/Stiften zu arretieren. Die hintere Keilnut verfügt über einen Metallverschluss, der sich über der Schraube/dem Stift schließt.
- d) Sichern Sie die Innenschiene mithilfe der M3 x 0,5 x 6-mm-Kreuzschlitzschrauben an der Seite des Chassis, um ein Rutschen zu verhindern.
- e) Installieren Sie die zweite Innenschiene an der gegenüberliegenden Seite des Chassis und sichern Sie sie mit den anderen M3 x 0,5 x 6-mm-Schrauben.

Vorsicht

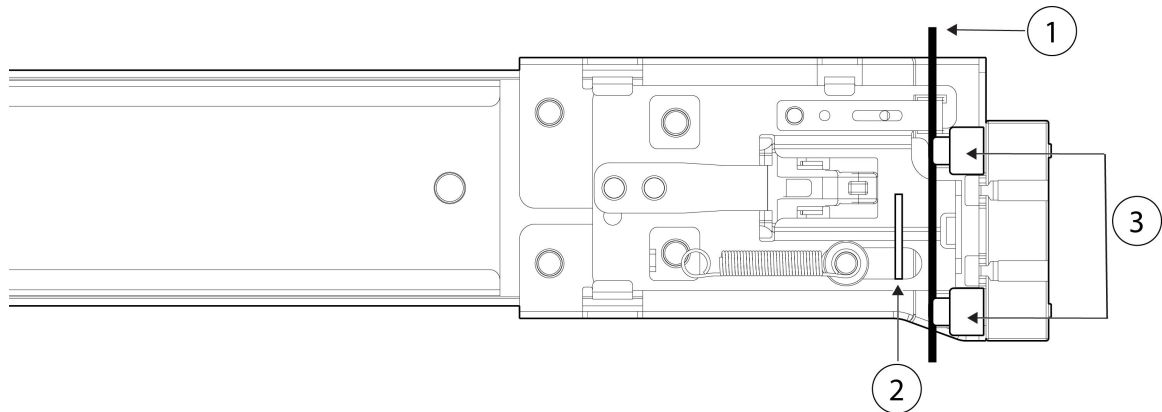
Aus Stabilitäts- und Sicherheitsgründen müssen die Schrauben immer an den Innenschienen installiert werden.

Schritt 4

Öffnen Sie die vordere Halterungsplatte an beiden Gleitschienen. Die Vorderseite der Gleitschiene verfügt über eine gefederte Halterungsplatte, die geöffnet werden muss, bevor Sie die Montagestifte in die Löcher der Rack-Säule stecken können.

Drücken Sie den grünen Pfeilknopf an der Außenseite der Baugruppe nach hinten, um die Halterungsplatte zu öffnen.

Abbildung 44: Vorderer Sicherungsmechanismus im Inneren der Vorderseite



1	Rack-Säule	2	Sicherungsplatte in nach hinten gezogener und geöffneter Position illustriert
3	Vordere Montagestifte Hinweis Geeignet für quadratische Steckplätze, 7,1 mm große Löchern und 10-32-Gewindelöcher		—

Schritt 5

Installieren der Gleitschienen im Rack:

- a) Richten Sie die Vorderseite einer Gleitschiene an den vorderen Rack-Säulenlöchern aus, die Sie verwenden möchten.

Die Vorderseite der Gleitschiene legt sich um die Außenseite der Rack-Säule und die Montagestifte werden von der Außenseite der Vorderseite in die Rack-Säulenlöcher gesteckt.

Hinweis

Die Rack-Säule muss sich zwischen den Montagestiften und der offenen Sicherungsplatte befinden.

- b) Schieben Sie die Montagestifte von der Außenseite der Vorderseite in die Rack-Säulenlöcher.
 c) Drücken Sie die Entriegelungstaste (mit Aufschrift „PUSH“) an der Halterungsplatte. Die federbelastete Halterungsplatte schließt sich, um die Stifte an Ort und Stelle zu verriegeln.
 d) Passen Sie die Länge der Gleitschiene an und schieben Sie anschließend die hinteren Montagestifte in die entsprechenden Rack-Säulenlöcher. Die Gleitschiene muss von vorne nach hinten gerade sein.
 Die hinteren Montagestifte werden von der Innenseite der Rack-Säule in die Rack-Säulenlöcher gesteckt.
 e) Bringen Sie die zweite Gleitschiene an der gegenüberliegenden Seite des Racks an. Stellen Sie sicher, dass die beiden Gleitschienen sich auf der gleichen Höhe befinden und von vorne nach hinten gerade sind.
 f) Ziehen Sie die inneren Gleitschienen jeder Baugruppe zur Vorderseite des Racks bis zu den inneren Anschlägen heraus und rasten sie ein.

Schritt 6

Stecken Sie das Chassis in die Gleitschienen.

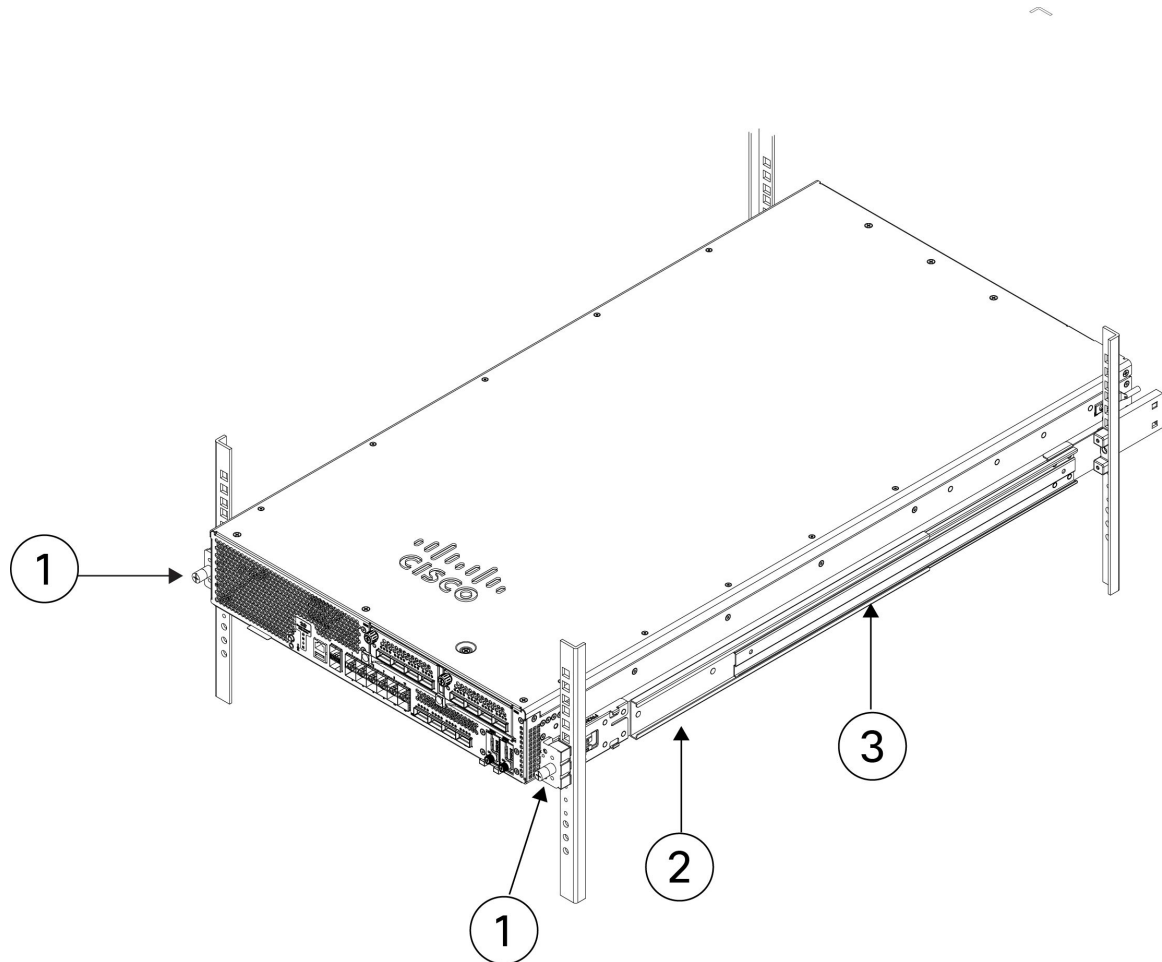
- a) Richten Sie die Rückseite der Innenschienen, die an den Seiten des Chassis angebracht sind, an den Vorderseiten der leeren Gleitschienen am Rack aus.
 b) Schieben Sie die Innenschienen bis zu den inneren Anschlägen in die Gleitschienen am Rack.

- c) Schieben Sie den Verriegelungsbügel zur Rückseite der beiden Innenschienen und schieben Sie anschließend das Chassis weiter in das Rack, bis die Montageklammern auf die Vorderseite der Gleitschiene treffen (siehe Abbildung unten).

Schritt 7

Sichern Sie das Chassis mithilfe der unverlierbaren Schrauben an der Vorderseite der Montageklammern vollständig am Rack.

Abbildung 45: Abgeschlossene Rackmontage



1	Unverlierbare Schrauben	2	Verriegelungsbügel der Innenschiene
3	Innenschiene an Chassis angebracht		—

Nächste Maßnahme

- Unter [Erdung des Chassis, auf Seite 85](#) finden Sie die Vorgehensweise zur Erdung der Secure Firewall 6100-Serie.
- Installieren Sie die Kabel gemäß Ihrer Softwarekonfiguration, wie in den [Leitfäden zu den ersten Schritten](#) beschrieben.

Erdung des Chassis



Hinweis Die Erdung des Chassis ist auch dann erforderlich, wenn das Rack bereits geerdet ist. Ein Erdungs-Kit zum Anbringen einer Erdungslasche wird mitgeliefert. Die Erdungslasche muss vom Nationally Recognized Testing Laboratory (NRTL) zugelassen sein. Außerdem muss ein Kupferleiter (Drähte) verwendet werden. Der Kupferleiter muss die vor Ort geltenden Anforderungen für Strombelastbarkeit erfüllen.

Das Erdungs-Pad befindet von den Netzteilen und Lüftern an der Rückseite gesehen aus auf der linken Seite des Chassis. Sie können eine Erdungslasche mit einem von Ihnen bereitgestellten Kabel befestigen.

Installationsvoraussetzungen für Erdungslaschen

Sie benötigen die folgenden Gegenstände, die Sie selbst bereitstellen:

- Verkabelungswerkzeug
- Crimpzange
- Erdungskabel
- Sie benötigen die folgenden Artikel aus dem Zubehör-Kit:
 - Eine Erdungslasche (6AWG, 0,25 Zoll)
 - Zwei Rundkopfschrauben (1/4-20 x 0,297-Zoll)
 - Zwei T-Unterlegscheiben mit 0,469 Zoll AD, 0,261 Zoll ID und 0,025 Zoll

Sicherheitswarnungen

Beachten Sie die folgenden Warnhinweise:



Warnung Anweisung 1024 – Erdungsleiter

Dieses Gerät muss geerdet sein. Auf keinen Fall den Erdungsleiter unwirksam machen oder das Gerät ohne einen sachgerecht installierten Erdungsleiter verwenden, um die Stromschlag- und Brandgefahr zu minimieren. Wenn Sie sich nicht sicher sind, ob eine sachgerechte Erdung vorhanden ist, wenden Sie sich an die zuständige Inspektionsbehörde oder einen Elektriker.



Warnung Anweisung 1046 – Installieren oder Ersetzen des Geräts

Beim Installieren oder Ersetzen des Geräts muss der Schutzleiter immer zuerst angeschlossen bzw. getrennt werden, um die Stromschlag- und Brandgefahr zu minimieren.

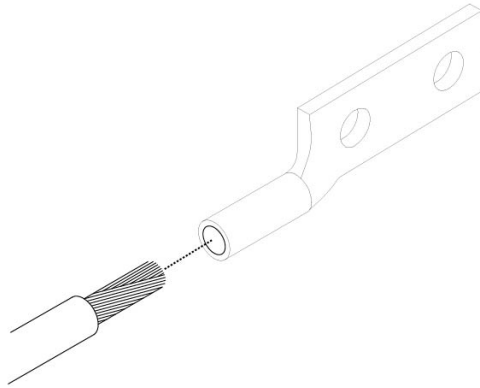
Wenn Ihr Gerät über Module verfügt, befestigen Sie diese mit den mitgelieferten Schrauben.

Prozedur

Schritt 1 Entfernen Sie mithilfe eines Abmantelwerkzeugs etwa 19 mm der Außenhülle vom Ende des Erdungskabels.

Schritt 2 Stecken Sie das abisolierte Ende des Erdungskabels in das offene Ende der Erdungslasche.

Abbildung 46: Einführen des Kabels in die Erdungslasche

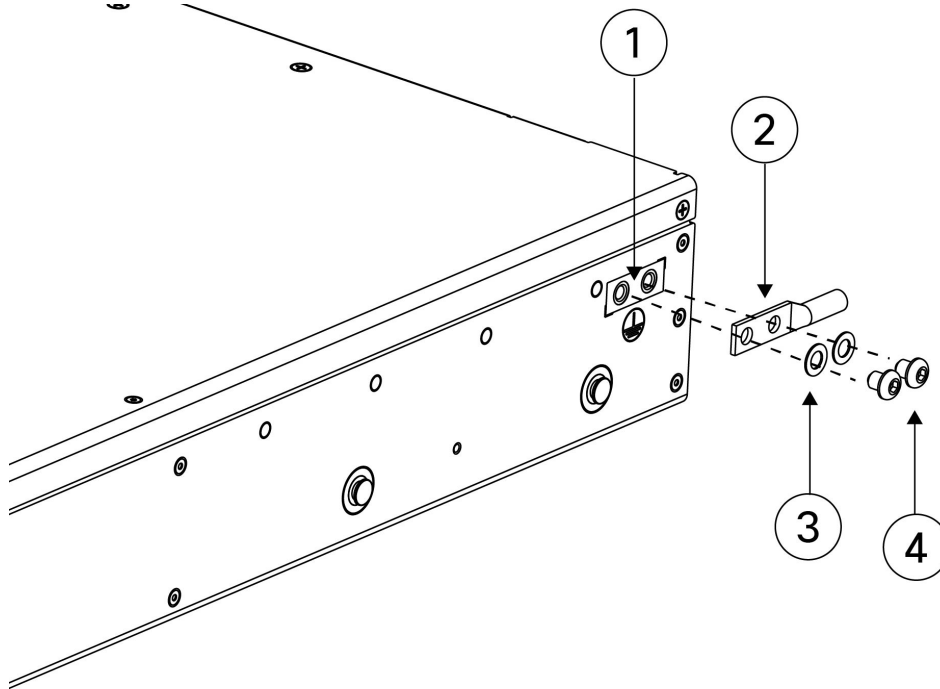


Schritt 3 Sichern Sie das Erdungskabel mithilfe der Crimpzange in der Erdungslasche.

Schritt 4 Entfernen Sie das Klebeetikett von der Erdungsplatte am Chassis.

Schritt 5 Befestigen Sie die Erdungslasche am Erdungs-Pad an der linken Seite des Chassis, sodass ein solider Kontakt der Metallflächen entsteht, und stecken Sie die beiden $\frac{1}{4}$ -20 x 0,297-Zoll-Rundkopfschrauben in das Erdungs-Pad.

Abbildung 47: Befestigen der Erdungslasche



1	Erdungs-Pad	2	Zwei interne Sicherungsscheiben
3	Von der Rückseite des Chassis aus gesehen auf der linken Seite	4	Zwei 1/4-20 x 0,297-Zoll-Rundkopfschrauben
5	Erdungsklemme		—

Schritt 6

Stellen Sie sicher, dass die Funktion anderer Geräte nicht durch die Lasche und das Kabel gestört wird.

Schritt 7

Präparieren Sie das andere Ende des Erdungskabels und verbinden Sie es mit einem geeigneten Erdungspunkt an Ihrem Standort, um eine angemessene Erdung zu gewährleisten.

Nächste Maßnahme

Installieren Sie die Kabel gemäß Ihrer Standard-Softwarekonfiguration, wie im [Leitfaden zu den ersten Schritten](#) beschrieben.



KAPITEL 4

Installation, Wartung und Upgrade

- [Installieren, Entfernen und Austauschen des Netzwerkmoduls, auf Seite 89](#)
- [Entfernen und Austauschen der SSD, auf Seite 91](#)
- [Entfernen und Austauschen des Lüftermoduls, auf Seite 92](#)
- [Entfernen und Austauschen des Netzteilmoduls, auf Seite 94](#)
- [Entfernen und Austauschen von DIMMs, auf Seite 96](#)

Installieren, Entfernen und Austauschen des Netzwerkmoduls

Sie können die Netzwerkmodule (NM-2 und NM-3) in der Secure Firewall 6100-Serie entfernen und austauschen. Obwohl die Hardware das Entfernen und Austauschen des Netzwerkmoduls im Systembetrieb unterstützt, wird die Hot-Swap-Funktion aktuell nicht durch die Software unterstützt. Sie müssen das Chassis ausschalten oder den Netzwerksteckplatz deaktivieren, um Netzwerkmodule zu entfernen und auszutauschen.

Informationen zum Management von Netzwerkmodulen finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

In diesem Verfahren wird beschrieben, wie Sie ein Netzwerkmodul in einem leeren Steckplatz installieren, in dem zuvor noch kein Netzwerkmodul installiert war, und wie Sie ein installiertes Netzwerkmodul entfernen und durch ein anderes Netzwerkmodul ersetzen.

Prozedur

Schritt 1

Gehen Sie wie folgt vor, um ein Netzwerkmodul zum ersten Mal in einem leeren Steckplatz zu installieren:

- a) Schalten Sie das Chassis aus, indem Sie die Power-Taste drücken.

Weitere Informationen zur Power-Taste finden Sie unter [Vorderseite, auf Seite 8](#). Informationen zum erstmaligen Installieren eines Netzwerkmoduls in einem leeren Steckplatz finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

- b) Befolgen Sie die Schritte 4 bis 7, um das neue Netzwerkmodul zu installieren.
- c) Schalten Sie das Chassis ein, indem Sie die Power-Taste drücken.

Schritt 2

Gehen Sie wie folgt vor, um ein vorhandenes Netzwerkmodul zu entfernen und zu ersetzen:

- a) Speichern Sie Ihre Konfiguration.

- b) Um ein vorhandenes Netzwerkmodul durch ein Netzwerkmodul desselben Modells zu ersetzen, deaktivieren Sie zunächst den Netzwerksteckplatz. Informationen zum Ersetzen eines vorhandenen Netzwerkmoduls durch ein Netzwerkmodul desselben Modells finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.
- c) Um ein vorhandenes Netzwerkmodul durch ein Netzwerkmodul eines anderen Modells zu ersetzen, schalten Sie das Chassis aus, indem Sie die Power-Taste in die Position „OFF“ (AUS) stellen. Informationen zum Ersetzen eines vorhandenen Netzwerkmoduls durch ein neues Modell finden Sie im Konfigurationsleitfaden für Ihr Betriebssystem.

Weitere Informationen zur Power-Taste finden Sie unter [Vorderseite, auf Seite 8](#).

- d) Fahren Sie mit Schritt 3 fort.

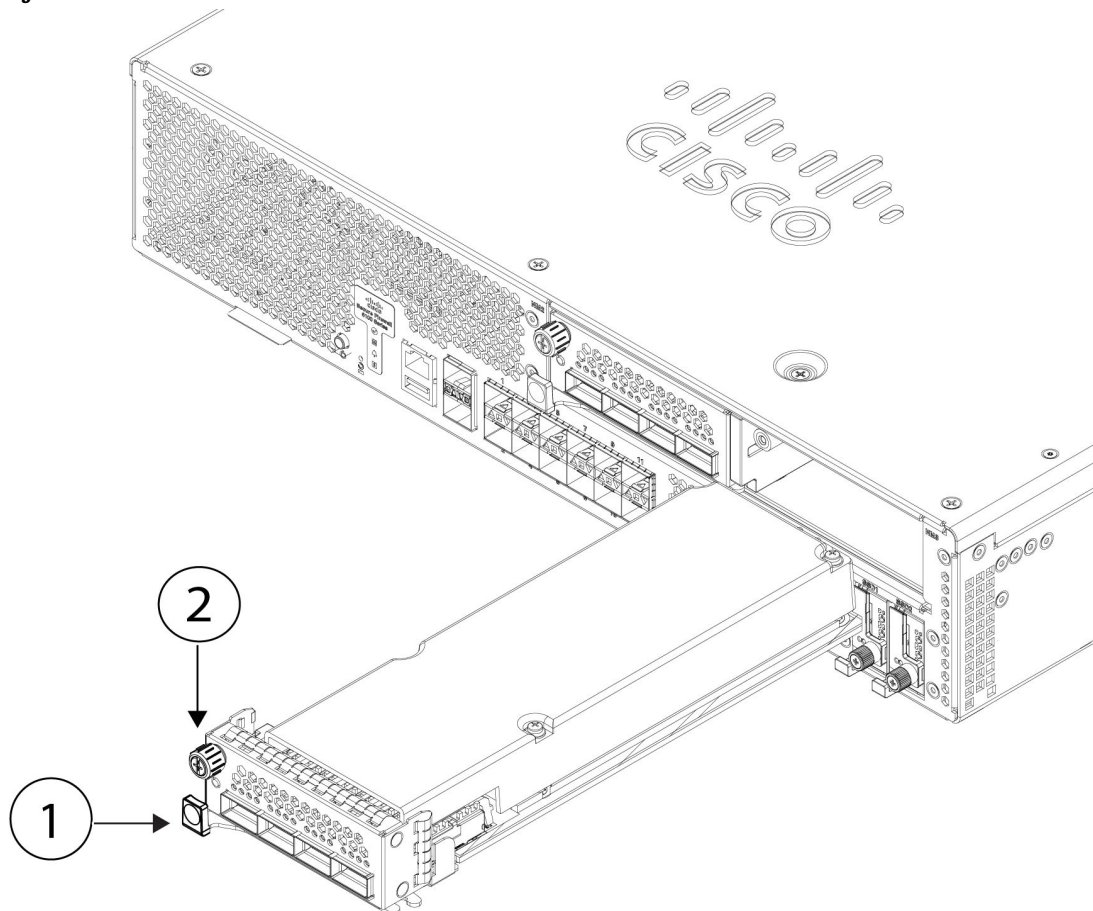
Schritt 3

Um ein Netzwerkmodul zu entfernen, lösen Sie die unverlierbare Schraube auf der oberen linken Seite des Netzwerkmoduls, drücken Sie den Auswurfhebel, und ziehen Sie den Hebel heraus. Damit wird das Netzwerkmodul mechanisch aus dem Steckplatz ausgeworfen.

Vorsicht

Die unverlierbare Schraube ist nicht am Hebel befestigt. Stellen Sie sicher, dass die unverlierbare Schraube vollständig gelöst ist, bevor Sie den Auswurfhebel herausziehen. Andernfalls können Sie den Auswurfhebel beschädigen, da sich die unverlierbare Schraube und der Hebel gegenseitig behindern.

Abbildung 48: Entfernen des Netzwerkmoduls



1	Auswurfhebel	2	Unverlierbare Schraube
----------	--------------	----------	------------------------

Falls der Steckplatz leer bleiben soll, installieren Sie eine leere Frontplatte, um eine ordnungsgemäße Luftzirkulation sicherzustellen und zu gewährleisten, dass kein Staub in das Chassis eindringt. Andernfalls installieren Sie ein anderes Netzwerkmodul.

- Schritt 4** Um ein Netzwerkmodul auszutauschen, halten Sie das Netzwerkmodul vor den Netzwerkmodulsteckplatz auf der rechten Seite des Chassis, drücken Sie den Auswurfhebel, und ziehen Sie den Hebel heraus.
- Schritt 5** Legen Sie das Netzwerkmodul in den Steckplatz, schieben Sie es fest hinein, und schließen Sie den Hebel auf der Vorderseite des Netzwerkmoduls.
- Schritt 6** Ziehen Sie die unverlierbare Schraube auf der oberen linken Seite des Netzwerkmoduls an.
- Schritt 7** Schalten Sie das Chassis ein, damit das neue Netzwerkmodul erkannt wird.

Entfernen und Austauschen der SSD

Das Chassis unterstützt zwei NVMe-SSDs. Die SSDs sind für SW-RAID1-Unterstützung konfiguriert. Weitere Informationen finden Sie unter [SSDs](#), auf Seite 32.

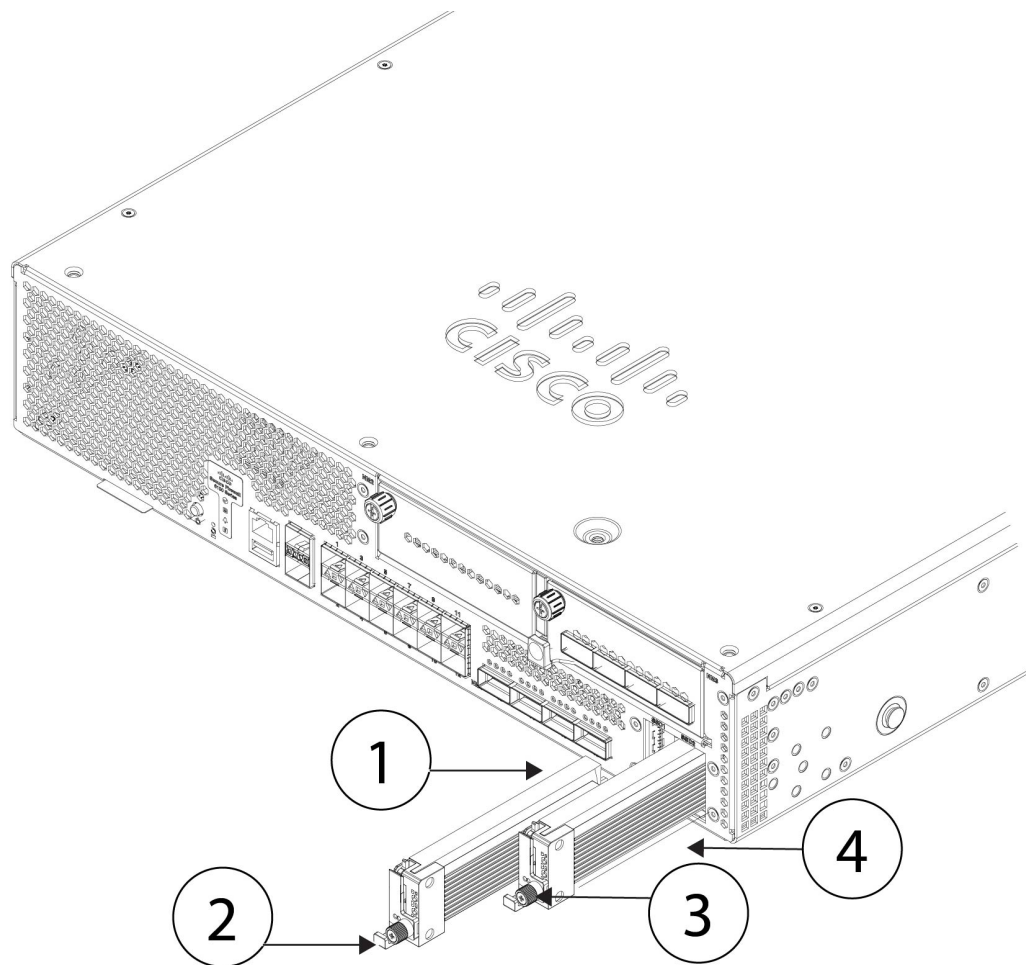


- Vorsicht** Der Austausch im laufenden Betrieb (Hot Swap) wird für die RAID-Konfiguration nicht unterstützt. Um eine SSD zu entfernen, müssen Sie sie mit dem Befehl **raid remove-secure local-disk 1|2** aus der RAID-Konfiguration löschen. Unter [Hot-Swapping einer SSD auf der Cisco Secure Firewall 3100/4200](#) finden Sie die Verfahren zum sicheren Entfernen einer SSD.

Prozedur

- Schritt 1** Speichern Sie Ihre Konfiguration.
- Schritt 2** Entfernen Sie SSD-1 oder SSD-2 mit dem Befehl **raid remove-secure local-disk 1|2** aus der RAID-Konfiguration.
- Schritt 3** Um die SSD aus dem Steckplatz zu entfernen, müssen Sie von der Vorderseite des Chassis aus die Arretierlasche an der Vorderseite der SSD zusammendrücken. Dadurch springt der Auswurfhebel auf.
- Schritt 4** Greifen Sie den Auswurfhebel, um die SSD vorsichtig aus dem Chassis zu ziehen.

Abbildung 49: Entfernen der SSD



1	SSD-1-Steckplatz	2	Griff
3	Unverlierbare Schraube	4	SSD-2-Steckplatz

- Schritt 5** Um SSD-1 oder SSD-2 wieder einzusetzen, halten Sie die SSD bei ausgezogenem Auswurfhebel vor den Steckplatz, drücken Sie sie vorsichtig hinein, bis sie einrastet, und schließen Sie dann den Auswurfhebel.
- Schritt 6** Prüfen Sie die LED der SSD, um sich zu vergewissern, ob die SSD betriebsbereit ist. Eine Beschreibung der SSD-LEDs finden Sie in Abschnitt [LEDs an der Vorderseite](#), auf Seite 12.
- Schritt 7** Fügen Sie die neue SSD mit dem Befehl `raid add local-disk 1|2` zur RAID-Konfiguration hinzu.

Entfernen und Austauschen des Lüftermoduls

Sie können die dualen Lüftermodule entfernen und austauschen, während das Chassis in Betrieb ist. Es sind vier Lüftermodule an der Rückseite des Chassis verbaut. Die Luft zirkuliert von der Vorderseite zur Rückseite

(E/A-Seite zu Nicht-E/A-Seite). Sie sind von links nach rechts auf der Rückseite des Chassis mit FAN-1 bis FAN-4 gekennzeichnet.



Vorsicht Durch das Entfernen aller Lüftermodule wird die Luftzirkulation im Chassis unterbrochen. Das Chassis kann nicht ordnungsgemäß eingeschaltet werden und hochfahren, wenn die Lüftermodule fehlen.



Vorsicht Wenn ein Lüftermodul ausfällt, entfernen Sie es aus dem Chassis und ersetzen Sie es innerhalb von 30 Sekunden. Nach 30 Sekunden kann die CPU-Temperatur die Betriebstemperatur überschreiten, was die Leistung beeinträchtigen kann.

Sicherheitswarnungen

Beachten Sie die folgenden Warnhinweise:



Warnung **Anweisung 1093** – Verletzungsgefahr durch scharfe Kanten

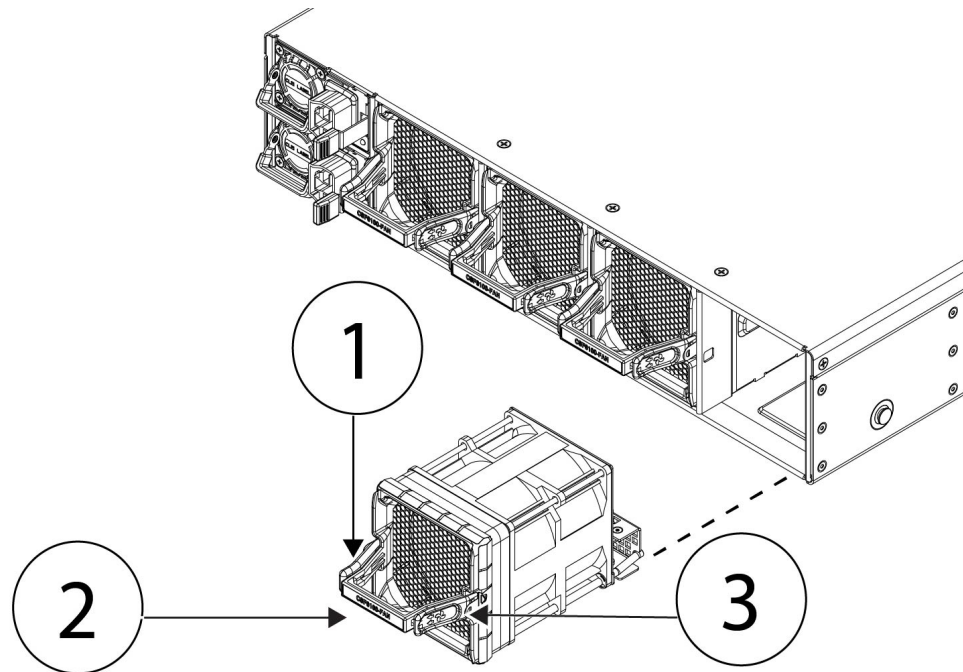
Risiko für Personenschäden. Es besteht Verletzungsgefahr an scharfen Kanten beim Installieren oder Entfernen von austauschbaren Einheiten.



Prozedur

-
- Schritt 1** Halten Sie das Lüftermodul für ein sofortiges Einsetzen in der Nähe des Chassis bereit, damit Sie es innerhalb von 30 Sekunden wieder einbauen können.
- Schritt 2** Um ein Lüftermodul zu entfernen, drücken Sie mit Blick auf die Rückseite des Chassis die Druckklaschen an den Seiten des Lüftermoduls, um es vom Chassis zu lösen.
- Schritt 3** Fassen Sie den Griff, und ziehen Sie das Lüftermodul aus dem Chassis heraus.

Abbildung 50: Entfernen des Lüftermoduls



1	Drucklasche	2	Griff
3	Drucklasche		—

Schritt 4

Um einen Lüftermodul auszutauschen, halten Sie es vor den Lüftersteckplatz.

Schritt 5

Drücken Sie die Druckklappen an den Seiten des Lüftermoduls und schieben Sie das Modul in das Chassis.

Schritt 6

Fassen Sie den Griff, und drücken Sie, bis das Lüftermodul richtig sitzt.

Falls das System eingeschaltet ist, hören Sie auf die Lüfter. Sie sollten den Betrieb der Lüfter unmittelbar hören können. Falls Sie die Lüfter nicht hören, stellen Sie sicher, dass das Lüftermodul vollständig in das Chassis eingelegt ist und die Frontplatte mit der Außenseite des Chassis bündig ist.

Schritt 7

Vergewissern Sie sich anhand der LED am Lüftermodul, ob der Lüfter betriebsbereit ist. Unter [Lüftermodule](#), auf [Seite 31](#) finden Sie eine Beschreibung der Lüfter-LEDs.

Entfernen und Austauschen des Netzteilmoduls

Netzteilmodule sind Hot-Swap-fähig. Sie können Netzteilmodule entfernen und austauschen, während das System in Betrieb ist. Der SAF-D-GRID-Anschluss dient als Trennvorrichtung für das AC/HVAC/HVDC-Netzteil.

Sicherheitswarnungen

Beachten Sie die folgenden Warnhinweise:



Warnung **Anweisung 1046** – Installieren oder Ersetzen des Geräts

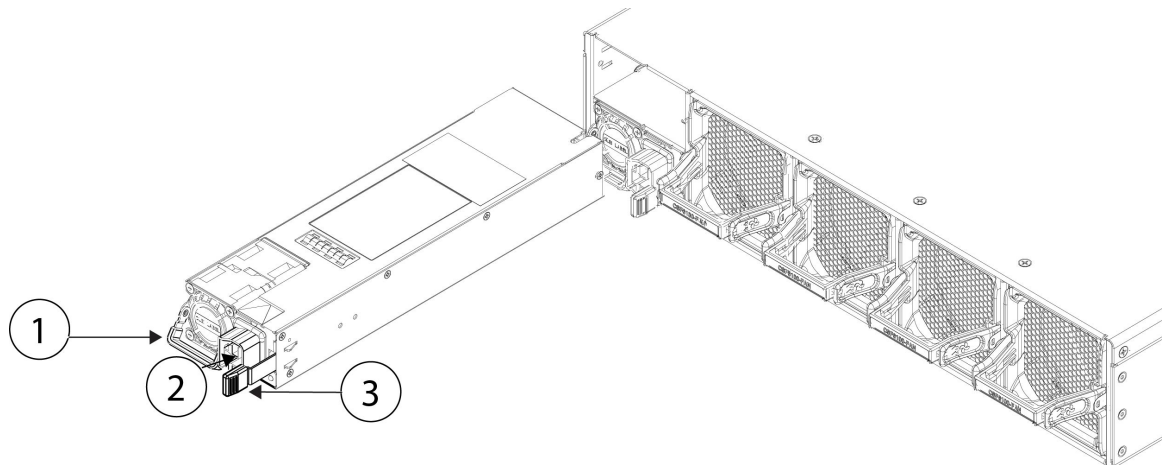
Beim Installieren oder Ersetzen des Geräts muss der Schutzleiter immer zuerst angeschlossen bzw. getrennt werden, um die Stromschlag- und Brandgefahr zu minimieren.

Wenn Ihr Gerät über Module verfügt, befestigen Sie diese mit den mitgelieferten Schrauben.

Prozedur

- Schritt 1** Ziehen Sie das Netzkabel ab, bevor Sie das Netzteilmodul entfernen. Sie können die Arretierlasche des Netzteilmoduls nicht lösen, ohne zuerst das Kabel zu entfernen.
- Schritt 2** Um ein Netzteilmodul zu entfernen, sehen Sie auf die Rückseite des Chassis, und greifen Sie nach dem Griff.
- Schritt 3** Drücken Sie die Arretierlasche nach links, um das Netzteil zu lösen. Die Arretierlasche befindet sich auf der rechten Seite des Netzteils.
- Schritt 4** Legen Sie Ihre andere Hand unter das Netzteilmodul, um es zu stützen, während Sie es aus dem Chassis ziehen.

Abbildung 51: Entfernen des Netzteilmoduls



1	Griff	2	Netzanschluss
3	Arretierlasche		—

Falls der Steckplatz leer bleiben soll, installieren Sie eine leere Frontplatte, um eine ordnungsgemäße Luftzirkulation sicherzustellen. Andernfalls installieren Sie ein anderes Netzteilmodul.

- Schritt 5** Zum Austauschen eines Netzteilmoduls halten Sie das Netzteilmodul mit beiden Händen fest und schieben es in den Netzteilmodulschacht.
- Schritt 6** Drücken Sie das Netzteilmodul vorsichtig hinein, bis Sie hören, wie die Arretierlasche einrastet, und merken, dass das Netzteil fest sitzt.
- Schritt 7** Stecken Sie das Netzkabel ein.

Schritt 8

Prüfen Sie die LED am Netzteilmodul, um sicherzustellen, dass das Netzteil funktionsfähig ist. Unter [Netzstrommodule](#), auf Seite 29 finden Sie eine Beschreibung der LED des Netzteilmoduls.

Entfernen und Austauschen von DIMMs

In diesem Verfahren wird beschrieben, wie Sie fehlerhafte DIMMs in der Secure Firewall 6100-Serie entfernen und ersetzen. DIMM-bezogene Fehler werden beim Start identifiziert. Zu diesem Zeitpunkt wird das System in den Fail-Safe-Modus versetzt. Sie können die Kommandozeile (CLI) verwenden, um fehlerhafte DIMMs zu identifizieren, wie unten dargestellt.

**Hinweis**

Sie können Ersatz-DIMMs nicht direkt bestellen. Sie müssen das TAC konsultieren, um die neuen DIMMs zu erhalten, damit Ihre Garantie nicht erlischt.

**Vorsicht**

Um Schäden durch elektrostatische Entladung zu vermeiden, tragen Sie bei diesem Verfahren Erdungsarmbänder, und fassen Sie die DIMMs nur an den Trägerkanten an.

Identifizieren fehlerhafter DIMMs

Verwenden Sie den CLI-Befehl **show dimm detail**, um zu ermitteln, welche DIMMs fehlerhaft sind. Wenn beim Booten ein DIMM-Ausfall erkannt wird, werden Sie feststellen, dass dieser in der DIMM-Liste fehlt. Das folgende Beispiel zeigt, dass keine DIMMs ausgefallen sind. Alle 24 DIMMs sind in beiden CPUs aufgeführt.

Diese Beispielausgabe wird nur auf der seriellen Konsole angezeigt, wenn ROMMON gestartet wird.

```
firepower-6160# scope server
firepower-6160 /chassis/server # scope memory-array 1
firepower-6160 /chassis/server/memory-array # show dimm detail
DIMMs installed:
CPU1 CHANNEL A CPU1 CHANNEL B CPU1 CHANNEL C CPU1 CHANNEL D CPU1 CHANNEL E CPU1 CHANNEL
F
CPU1 CHANNEL G CPU1 CHANNEL H CPU1 CHANNEL I CPU1 CHANNEL J CPU1 CHANNEL K CPU1 CHANNEL
L
CPU2 CHANNEL A CPU2 CHANNEL B CPU2 CHANNEL C CPU2 CHANNEL D CPU2 CHANNEL E CPU2 CHANNEL
F
CPU2 CHANNEL G CPU2 CHANNEL H CPU2 CHANNEL I CPU2 CHANNEL J CPU2 CHANNEL K CPU2 CHANNEL
L
```

Das folgende Beispiel zeigt, dass ein DIMM-Ausfall aufgetreten ist. CPU1 CHANNEL L is missing.

```
DIMMs installed:
CPU1 CHANNEL A CPU1 CHANNEL B CPU1 CHANNEL C CPU1 CHANNEL D CPU1 CHANNEL E CPU1 CHANNEL
F
CPU1 CHANNEL G CPU1 CHANNEL H CPU1 CHANNEL I CPU1 CHANNEL J CPU1 CHANNEL K
CPU2 CHANNEL A CPU2 CHANNEL B CPU2 CHANNEL C CPU2 CHANNEL D CPU2 CHANNEL E CPU2 CHANNEL
F
CPU2 CHANNEL G CPU2 CHANNEL H CPU2 CHANNEL I CPU2 CHANNEL J CPU2 CHANNEL K CPU2 CHANNEL
L
WARNING: This system needs more memory device(s). Expected 24, installed 23
%WARNING% - Please correct the memory issue to assure best performance.
```

Sicherheitswarnungen

Beachten Sie die folgenden Warnhinweise:



Warnung **Anweisung 1093** – Verletzungsgefahr durch scharfe Kanten

Risiko für Personenschäden. Es besteht Verletzungsgefahr an scharfen Kanten beim Installieren oder Entfernen von austauschbaren Einheiten.



Gehen Sie wie folgt vor, um ein fehlerhaftes DIMM aus dem Secure Firewall 6100-Chassis zu entfernen und zu ersetzen:



Vorsicht DIMMs und ihre Steckplätze sind empfindlich und müssen mit Vorsicht gehandhabt werden, um Schäden während der Installation zu vermeiden.



Vorsicht Cisco unterstützt keine DIMMs von Drittanbietern. Die Verwendung von DIMMs, die nicht von Cisco stammen, kann zu Systemproblemen oder Schäden an der internen Platine führen.

Vorbereitungen

- Wenden Sie sich an das TAC, um den Ausfall von DIMMs zu überprüfen und Ersatz-DIMM(s) zu erhalten.
- Planen Sie nach Erhalt der Ersatz-DIMMs ein Wartungsfenster für die betroffene Secure Firewall 6100-Serie.
- Halten Sie für den Vorgang ein ESD-Armband und eine ESD-Matte bereit.
- Entfernen Sie alle Stromquellen vom Chassis.



Hinweis Unter [Power-Taste und Reset-Taste, auf Seite 9](#) finden Sie das Verfahren zum Ausschalten des Chassis.

- Entfernen Sie das Chassis aus dem Rack.

Prozedur

-
- Schritt 1** Notieren Sie sich die CPU- und Kanalbezeichnung für das/die fehlerhafte(n) DIMM-Modul(e).
- Schritt 2** Entfernen Sie alle Stromquellen vom Chassis.

Trennen Sie bei Wechselstromsystemen den AC-Eingang vom Netzteilmodul.

Schalten Sie bei Gleichstromsystemen den Trennschalter oder Schutzschalter aus und entfernen Sie das Netzteilmodul aus dem Chassis.

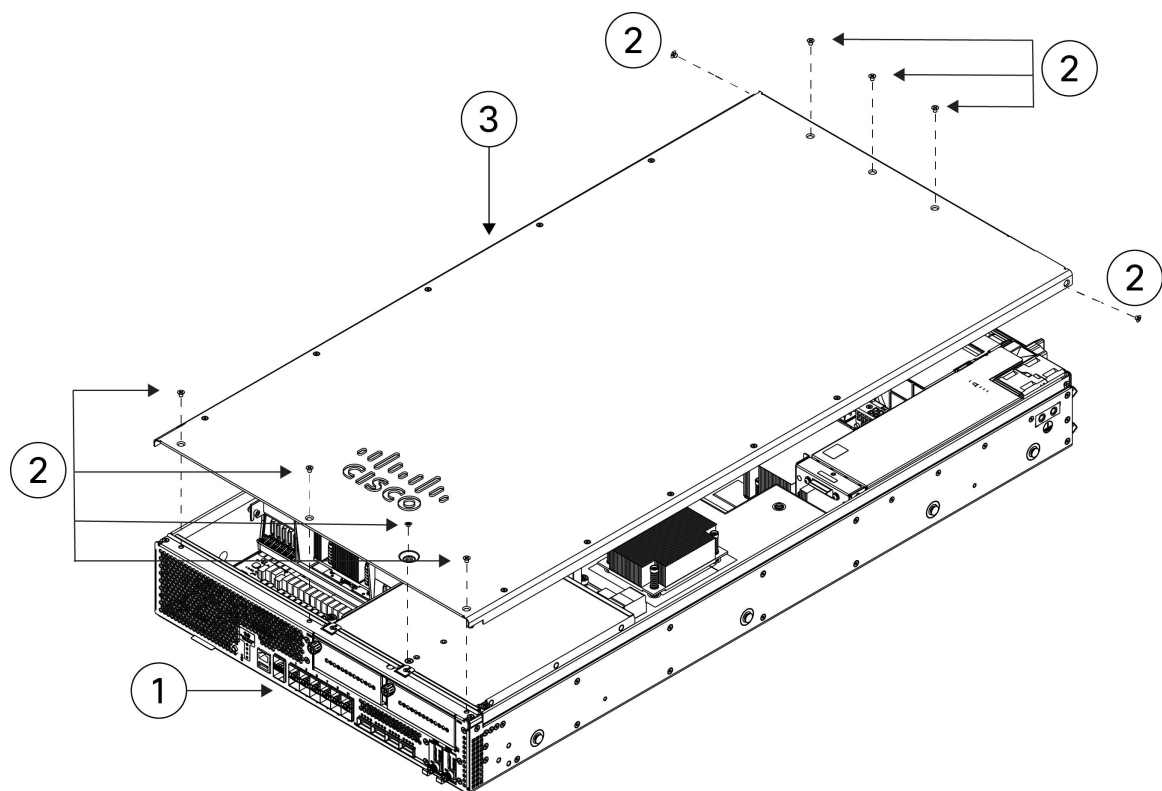
Schritt 3 Entfernen Sie das Chassis aus dem Rack.

Unter [Rackmontage des Chassis mit Gleitschienen, auf Seite 78](#) finden Sie das Verfahren zum Entfernen des Chassis aus dem Rack.

Schritt 4 Stellen Sie das Chassis auf eine antistatische Matte.

Schritt 5 Entfernen Sie die sieben Schrauben von der Oberseite der Chassis-Abdeckung und die zwei Schrauben an den Seiten. Ziehen Sie die Abdeckung nach oben und vom Chassis ab.

Abbildung 52: Entfernen der Chassis-Abdeckung

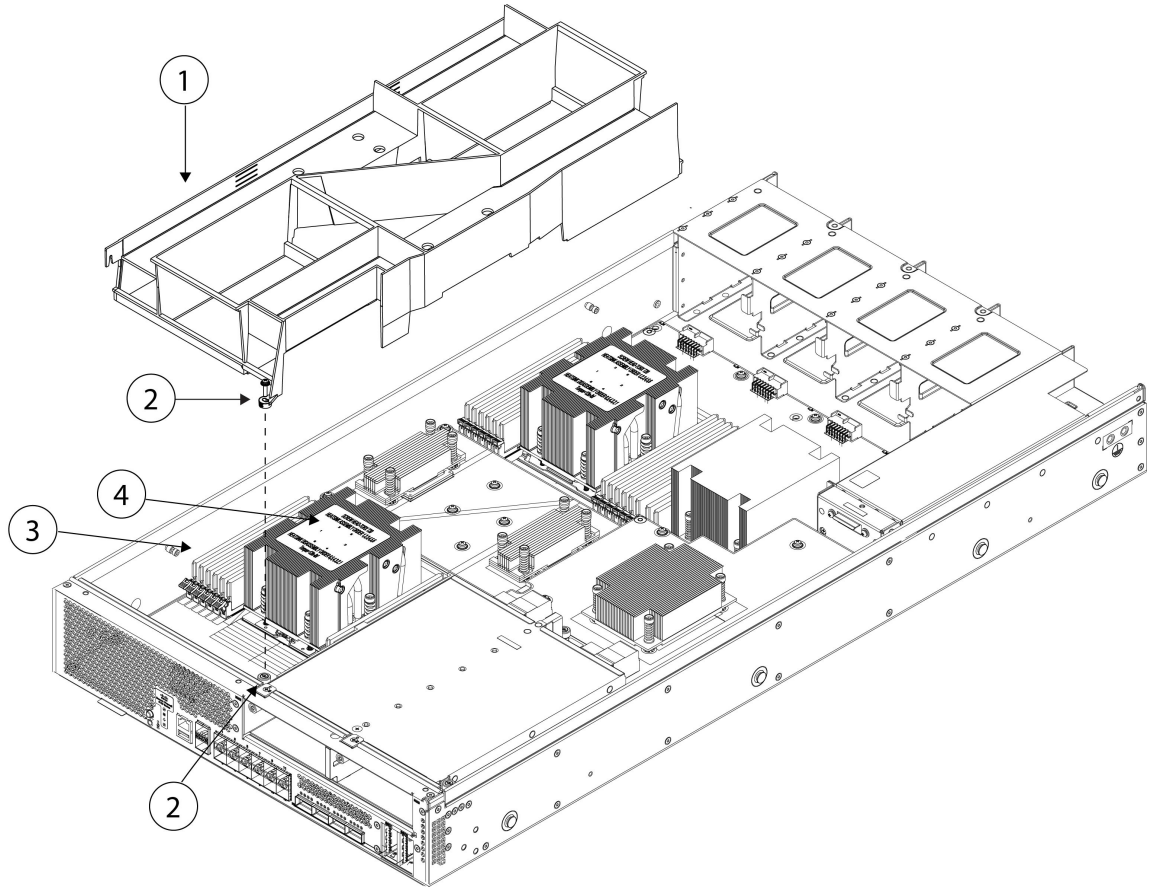


1	Vorderseite (E/A-Seite)	2	Schrauben der Chassis-Abdeckung (9)
3	Chassis-Abdeckung		—

Schritt 6 Entfernen Sie die Schraube am Leitblech und heben es an und heraus.

Das Leitblech umfasst die oberen DIMM-Bänke und die beiden CPUs.

Abbildung 53: Entfernen des Leitblechs von der internen Platine



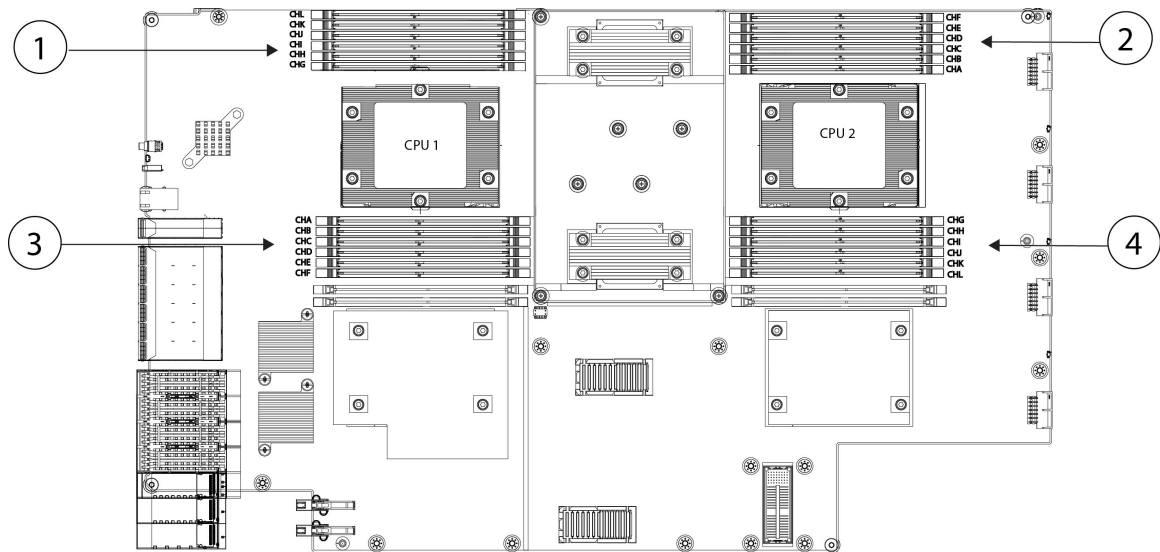
1	Leitblech	2	Leitblechschraube
3	DIMM-Bank	4	CPU 1

Schritt 7

Lokalisieren Sie das DIMM, das Sie entfernen möchten, auf der internen Platine.

Es gibt vier DIMM-Bänke mit sechs DIMM-Steckplätzen pro Bank.

Abbildung 54: DIMM-Bänke auf der internen Platine

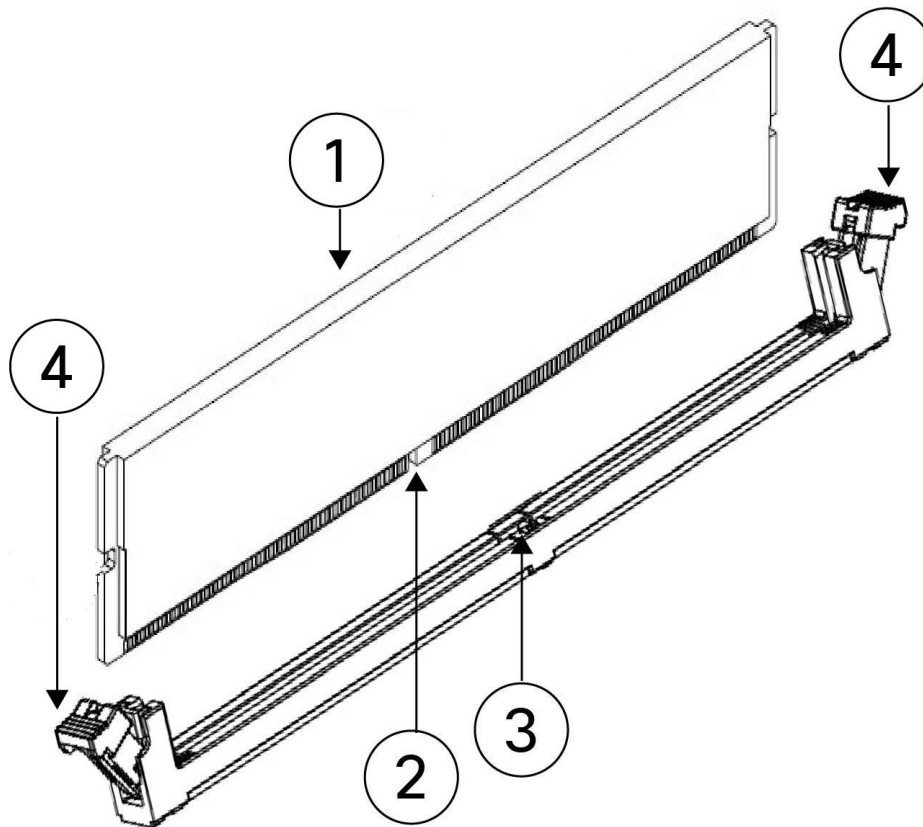


1	DIMM-Bank mit den Kanälen L, K, J, I, H, G	2	DIMM-Bank mit den Kanälen F, E, D, C, B, A
3	DIMM-Bank mit den Kanälen A, B, C, D, E, F	4	DIMM-Bank mit den Kanälen G, H, I, J, K, L

Schritt 8

Öffnen Sie die DIMM-Steckplatzverriegelungen, indem Sie die Auswurfhebel an beiden Enden des Steckplatzes nach unten drücken; ziehen Sie das DIMM nach oben und heraus.

Abbildung 55: Öffnen der DIMM-Steckplatzverriegelungen



1	DIMM	2	DIMM-Kerbe
3	DIMM-Steckplatzkerbe	4	Öffnen der DIMM-Steckplatzverriegelungen

Schritt 9 Richten Sie das neue DIMM am leeren Steckplatz auf der internen Platine des Chassis aus. Verwenden Sie die Ausrichtungshilfe im DIMM-Steckplatz, um das DIMM korrekt auszurichten.

Hinweis

Achten Sie darauf, dass die Kerbe im DIMM am Steckplatz ausgerichtet ist. Bei falscher Ausrichtung des Steckplatzes können das DIMM oder der Steckplatz beschädigt werden.

Schritt 10 Drücken Sie die oberen beiden Enden des DIMM-Moduls gleichmäßig nach unten, bis es vollständig eingesetzt ist und die Auswurfhebel an beiden Enden des DIMM-Moduls einrasten.

Schritt 11 Senken Sie das Leitblech wieder ab und ziehen Sie die Schraube fest (siehe Abbildung *Entfernen des Leitblechs von der internen Platine* oben).

Schritt 12 Setzen Sie die Chassis-Abdeckung wieder ein und ziehen Sie die neun Schrauben fest (siehe Abbildung *Entfernen der Chassis-Abdeckung* oben).

Schritt 13 Installieren Sie das Chassis im Rack.

Unter [Rackmontage des Chassis mit Gleitschienen, auf Seite 78](#) finden Sie das Verfahren zum Entfernen des Chassis aus dem Rack.

Schritt 14

Schließen Sie die Netzteilmodule an.

Schritt 15

Schalten Sie die Secure Firewall 6100 wieder online.

Anweisungen, wie Sie das Chassis wieder online schalten, finden Sie im FXOS-Konfigurationsleitfaden für Ihre Softwareversion.

Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.