

FTD: Aktivieren der TCP-State-Bypass-Konfiguration mithilfe der FlexConfig-Richtlinie

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Schritt 1: Konfigurieren eines Extended Access List-Objekts](#)

[Schritt 2: Konfigurieren eines FlexConfig-Objekts](#)

[Schritt 3: Zuweisen einer FlexConfig-Richtlinie zum FTD](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Verwandte Links](#)

Einführung

In diesem Dokument wird beschrieben, wie die Transmission Control Protocol (TCP) State Bypass-Funktion auf FirePOWER Threat Defense (FTD)-Appliances über FirePOWER Management Center (FMC) mithilfe der FlexConfig Policy in Versionen vor 6.3.0 implementiert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse des FirePOWER Management Center.
- Grundlegende Kenntnisse des FirePOWER Threat Defense.
- Informationen über die Funktion zum Umgehen des TCP-Zustands.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Firepower Threat Defense (FTD) Version 6.2.3.
- FirePOWER Management Center (FMC) Version 6.2.3

Hintergrundinformationen

TCP State Bypass ist eine von der Adaptive Security Appliance (ASA) geerbte Funktion und bietet Unterstützung bei der Fehlerbehebung von Datenverkehr, der entweder durch TCP-Normalisierungsfunktionen, asymmetrische Routing-Bedingungen und bestimmte Anwendungsinspektionen verworfen werden könnte.

Diese Funktion wird nativ auf FMC ab Version 6.3.0 unterstützt. Es wird empfohlen, die Flexconfig-Objekte nach dem Upgrade zu löschen und diese Konfiguration vor der ersten Bereitstellung auf das FMC zu verschieben. Weitere Informationen zum Konfigurieren von TCP-State-Bypass in Version 6.3.0 oder höher finden Sie in diesem [Konfigurationsleitfaden](#).

FirePOWER Threat Defense verwendet ASA-Konfigurationsbefehle, um einige Funktionen, aber nicht alle Funktionen zu implementieren. Es gibt keine eindeutigen Konfigurationsbefehle für FirePOWER Threat Defense. FlexConfig ermöglicht Ihnen stattdessen die Konfiguration von Funktionen, die noch nicht direkt durch die Richtlinien und Einstellungen von Firepower Management Center unterstützt werden.

Hinweis: TCP-Zustandsumgehung sollte nur zu Fehlerbehebungszwecken verwendet werden oder wenn asymmetrisches Routing nicht aufgelöst werden kann. Die Verwendung dieser Funktion deaktiviert mehrere Sicherheitsfunktionen und kann bei unzureichender Implementierung zu einer hohen Anzahl von Verbindungen führen.

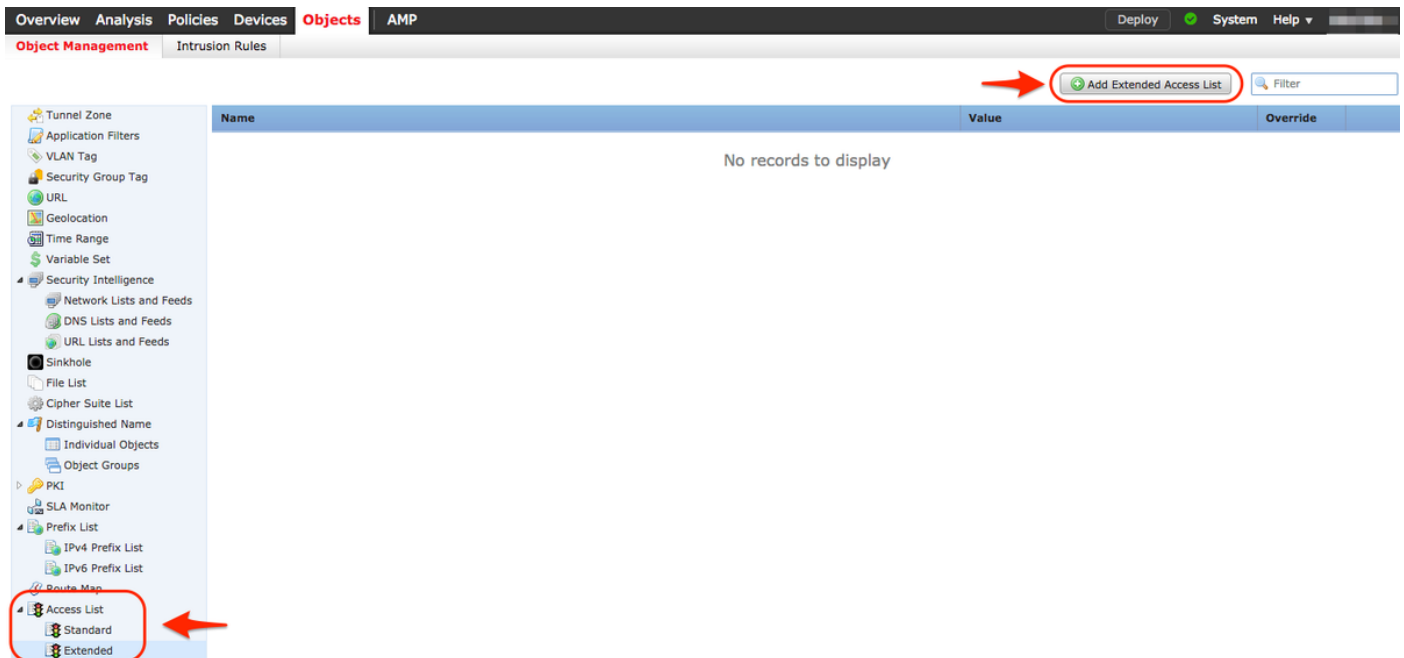
Weitere Informationen zur TCP-State-Bypass-Funktion oder deren Implementierung in ASA finden Sie im [Konfigurationshandbuch](#) zur [Konfiguration der TCP-State-Bypass-Funktion auf der ASA 5500-Serie](#) und im Konfigurationshandbuch zur Cisco Serie ASA 5500.

Konfiguration

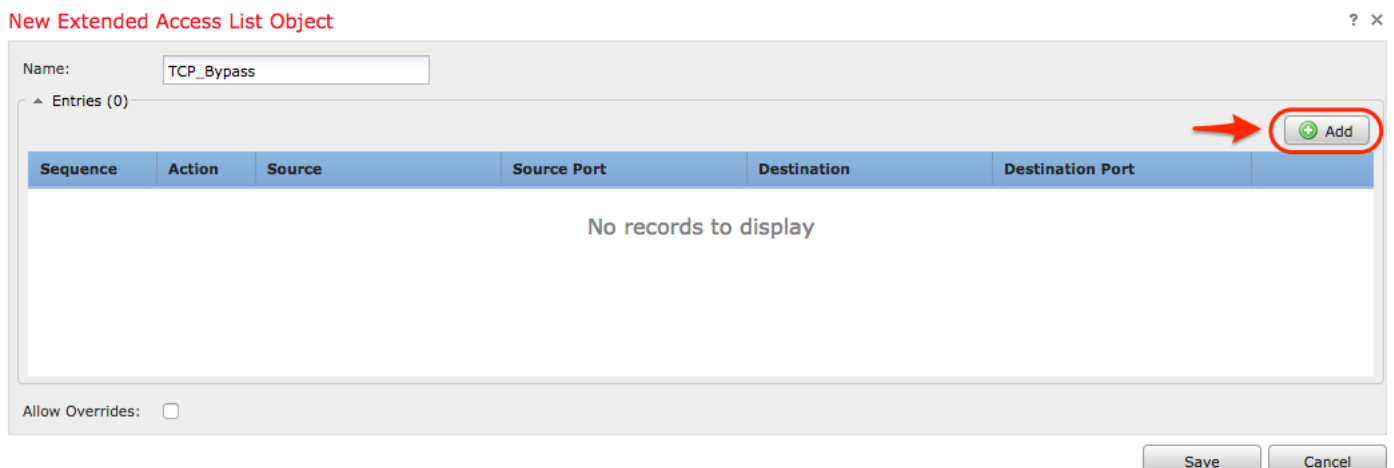
In diesem Abschnitt wird beschrieben, wie der TCP-State-Bypass auf dem FMC mithilfe einer FlexConfig-Richtlinie konfiguriert wird.

Schritt 1: Konfigurieren eines Extended Access List-Objekts

Um eine erweiterte Zugriffsliste auf dem FMC zu erstellen, gehen Sie zu **Objekte > Objektmanagement** und klicken Sie im linken Menü unter **Zugriffsliste** auf **Erweitert**. Klicken Sie auf Erweiterte Zugriffsliste hinzufügen.



Füllen Sie das Feld Name mit dem gewünschten Wert aus. in diesem Beispiel lautet der Name **TCP_Bypass**. Klicken Sie auf Schaltfläche **Hinzufügen**.



Die Aktion für diese Regel muss als **Zulassen** konfiguriert werden. Es kann ein systemdefiniertes Netzwerk verwendet oder für jede Quelle und jedes Ziel ein neues Netzwerkobjekt erstellt werden. In diesem Beispiel ordnet die Zugriffsliste IP-Datenverkehr von Host1 zu Host2 zu, da dies die Kommunikation zur Anwendung von TCP-State-Bypass ist. Die Registerkarte "Port" kann optional verwendet werden, um einen bestimmten TCP- oder UDP-Port zuzuordnen. Klicken Sie auf die Schaltfläche **Hinzufügen**, um fortzufahren.

Add Extended Access List Entry

? x

Action: Allow

Logging: Default

Log Level: Informational

Log Interval: Sec.

Network Port

Available Networks

- any
- any-ipv4
- any-ipv6
- FMC
- Host1
- Host2
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

Add to Source

Add to Destination

Source Networks (1)

- Host1

Destination Networks (1)

- Host2

Enter an IP address Add

Enter an IP address Add

Add Cancel

Wenn Sie die Quell- und Zielnetzwerke oder -Hosts ausgewählt haben, klicken Sie auf **Speichern**.

Edit Extended Access List Object

? x

Name:

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	
1	<input checked="" type="checkbox"/> Allow	Host1	Any	Host2	Any	<input type="checkbox"/> <input type="checkbox"/>

Allow Overrides:

Save Cancel

Schritt 2: Konfigurieren eines FlexConfig-Objekts

Navigieren Sie zu **Objekte > Objektmanagement > FlexConfig > FlexConfig Object**, und klicken Sie auf die Schaltfläche **FlexConfig-Objekt** hinzufügen.

Overview Analysis Policies Devices **Objects** AMP Deploy System Help

Object Management Intrusion Rules

Add FlexConfig Object Filter

Name	Description
Default_DNS_Configure	Configure Default DNS with the help of TextObjects default
Default_Inspection_Protocol_Disable	Disable Default Inspection.
Default_Inspection_Protocol_Enable	Enable Default Inspection.
DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface
DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one i
DNS_Configure	Configure DNS with the help of TextObjects dnsParameter
DNS_UnConfigure	Remove the DNS configurations.
Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures au
Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures a
Eigrp_UnConfigure	Clears eigrp configuration for an AS
Eigrp_Unconfigure_All	Clears eigrp configuration.
Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in t
Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.
ISIS_Configure	Configures global parameters for IS-IS.
ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv6
ISIS_Unconfigure	Unconfigures is-is.
ISIS_Unconfigure_All	Unconfigures is-is.
Netflow_Add_Destination	Create and configure a NetFlow export destination.
Netflow_Clear_Parameters	Set NetFlow export global settings back to default values.

Displaying 1 - 20 of 48 rows Page 1 of 3

Der Name des Objekts für dieses Beispiel heißt **TCP_Bypass** genau wie die Zugriffsliste. Dieser Name muss nicht mit dem Namen der Zugriffsliste übereinstimmen.

Wählen Sie **Policy Object einfügen > Extended ACL Object** aus.

Add FlexConfig Object ? x

Name: TCP_Bypass

Description: TCP State Bypass

Deployment: **Everytime** Type: Append

- Insert Policy Object
 - Text Object
 - Network
 - Security Zones
 - Standard ACL Object
 - Extended ACL Object**
 - Route Map
- Insert System Variable
- Insert Secret Key

Variables

Name	Dimension	Default Value	Property (Ty...	Override	Description
No records to display					

Save Cancel

Hinweis: Wählen Sie die Option "Everytime" aus. Dadurch kann diese Konfiguration auch bei

anderen Bereitstellungen und Upgrades beibehalten werden.

Wählen Sie im Abschnitt **Verfügbare Objekte** die in Schritt 1 erstellte Zugriffsliste aus, und weisen Sie einen Variablennamen zu. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**. In diesem Beispiel lautet der Variablenname **TCP_Bypass**.

Klicken Sie auf **Speichern**.

Insert Extended Access List Object Variable

The screenshot shows a dialog box titled "Insert Extended Access List Object Variable". It has a "Variable Name:" field with "TCP_Bypass" and an empty "Description:" field. Below are two panes: "Available Objects" with a search bar and a list containing "TCP_Bypass" (highlighted), and "Selected Object" with a list containing "TCP_Bypass". An "Add" button is between the panes. At the bottom right are "Save" and "Cancel" buttons.

Fügen Sie die nächsten Konfigurationszeilen im leeren Feld direkt unter der Schaltfläche **Einfügen** hinzu, und fügen Sie die zuvor definierte Variable (**\$TCP_Bypass**) in die Konfigurationszeile Match-Zugriffsliste ein. Beachten Sie, dass ein **\$**-Symbol dem Variablennamen vorangestellt wird. Dies hilft zu definieren, dass eine Variable danach folgt.

```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

In diesem Beispiel wird eine Richtlinienzuordnung erstellt und auf die externe Schnittstelle angewendet. Wenn der TCP-State-Bypass als Teil der globalen Dienstrichtlinie konfiguriert werden muss, kann die Klassenzuordnung "tcp_bypass" auf global_policy angewendet werden.

Klicken Sie abschließend auf **Speichern**.

Add FlexConfig Object

Name:

Description:

Deployment: Type:

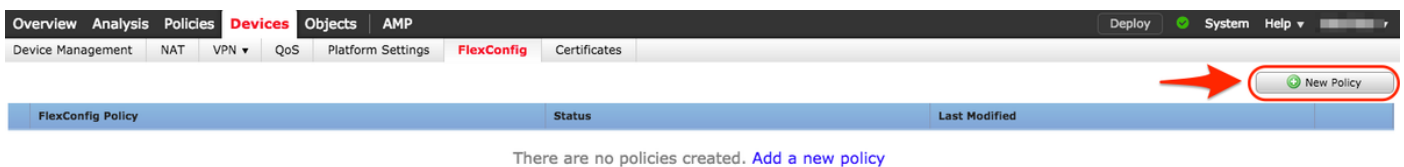
```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

Variables

Name	Dimension	Default Value	Property (Ty...	Override	Description
No records to display					

Schritt 3: Zuweisen einer FlexConfig-Richtlinie zum FTD

Gehen Sie zu **Devices > FlexConfig**, und erstellen Sie eine neue Richtlinie (es sei denn, es wurde bereits eine Richtlinie für einen anderen Zweck erstellt und derselben FTD zugewiesen). In diesem Beispiel wird die neue FlexConfig-Richtlinie als **TCP_Bypass** bezeichnet.



Weisen Sie dem FTD-Gerät die **TCP_Bypass** FlexConfig-Richtlinie zu.

New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTD

Selected Devices

FTD

Wählen Sie das FlexConfig-Objekt mit dem Namen **TCP_Bypass** aus, das in Schritt 2 unter dem Abschnitt **User Defined** erstellt wurde, und klicken Sie auf den Pfeil, um dieses Objekt der Richtlinie hinzuzufügen.

Overview Analysis Policies **Devices** Objects AMP Deploy System Help

Device Management NAT VPN QoS Platform Settings **FlexConfig** Certificates

TCP_Bypass You have unsaved changes Preview Config Save Cancel

TCP State Bypass Policy Assignments (1)

Available FlexConfig FlexConfig Object

- User Defined
 - TCP_Bypass**
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure
 - DNS_Configure
 - DNS_UnConfigure
 - Eigrp_Configure
 - Eigrp_Interface_Configure
 - Eigrp_UnConfigure
 - Eigrp_Unconfigure_All
 - Inspect_IPv6_Configure
 - Inspect_IPv6_UnConfigure
 - ISIS_Configure
 - ISIS_Interface_Configuration
 - ISIS_Unconfigure
 - ISIS_Unconfigure_All
 - Netflow_Add_Destination
 - Netflow_Clear_Parameters

Selected Prepend FlexConfigs

#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
1	TCP_Bypass	TCP State Bypass

Speichern und Bereitstellen der Änderungen

Deploy Policies Version: 2017-08-22 12:02 PM ? X

Device	Group	Current Version
<input checked="" type="checkbox"/> <input type="checkbox"/> FTD		2017-08-18 01:06 AM

- Nat Policy: NAT-Lab
- NGFW Settings: Platform_Lab
- FlexConfig Policy: TCP_Bypass
- Access Control Policy: Policy_FTD
- Intrusion Policy: Balanced Security and Connectivity
- DNS Policy: Default DNS Policy
- Prefilter Policy: Default Prefilter Policy
- Network Discovery
- Device Configuration ([Details](#))

Selected devices: 1

Überprüfung

Zugriff auf das FTD über SSH oder Konsole und Verwendung der **Diagnosesystemunterstützung**.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
firepower# show access-list TCP_Bypass
access-list TCP_Bypass; 1 elements; name hash: 0xec2b41eb
access-list TCP_Bypass line 1 extended permit object-group ProxySG_ExtendedACL_34359739205
object Host1 object Host2 log informational interval 300 (hitcnt=0) 0x42940b0e
access-list TCP_Bypass line 1 extended permit ip host 1.1.1.1 host 1.1.1.2 log informational
interval 300 (hitcnt=0) 0x769561fc
```

```
firepower# show running-config class-map
!
class-map inspection_default
match default-inspection-traffic
class-map tcp_bypass
match access-list TCP_Bypass
!
firepower# show running-config policy-map
```

```
!  
policy-map type inspect dns preset_dns_map  
parameters  
message-length maximum client auto  
message-length maximum 512  
no tcp-inspection  
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP  
parameters  
eool action allow  
nop action allow  
router-alert action allow  
policy-map global_policy  
class inspection_default  
inspect dns preset_dns_map  
inspect ftp  
inspect h323 h225  
inspect h323 ras  
inspect rsh  
inspect rtsp  
inspect sqlnet  
inspect skinny  
inspect sunrpc  
inspect xdmcp  
inspect sip  
inspect netbios  
inspect tftp  
inspect icmp  
inspect icmp error  
inspect ip-options UM_STATIC_IP_OPTIONS_MAP  
class class-default  
set connection advanced-options UM_STATIC_TCP_MAP  
policy-map tcp_bypass_policy  
class tcp_bypass  
set connection advanced-options tcp-state-bypass  
!
```

Fehlerbehebung

Zur Fehlerbehebung führen diese Befehle zu hilfreichen Ergebnissen.

- **show conn [detail]**

Shows connection information. Detailed information uses flags to indicate special connection characteristics.

For example, the "b" flag indicates traffic subject to TCP State Bypass

- **show service-policy**

Shows service policy statistics, including Dead Connection Detection (DCD) statistics

Verwandte Links

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_configuration/conns_connlimits.html

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118995-configure-asa-00.html>

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configuration-guide-v62/flexconfig_policies.html