

Konfigurieren des FQDN-basierten Objekts für Zugriffskontrollregeln

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Konfiguration des Fully Qualified Domain Name (FQDN)-Objekts über das Firewall Management Center (FMC) und die Verwendung des FQDN-Objekts bei der Erstellung von Zugriffsregeln.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der FirePOWER-Technologie
- Kenntnisse der Konfiguration der Zugriffskontrollrichtlinie für das FireSIGHT Management Center (FMC)

Verwendete Komponenten

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

- FirePOWER Management Center mit Version 6.3 und höher
- Firepower Threat Defense mit Version 6.3 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt 1: Um ein FQDN-basiertes Objekt zu konfigurieren und zu verwenden, konfigurieren Sie

zunächst DNS in FirePOWER Threat Defense.

Melden Sie sich beim FMC an, und navigieren Sie zu **Devices > Platform Settings > DNS**.

The screenshot shows the 'DNS Resolution Settings' configuration page. On the left is a navigation menu with options: ARP Inspection, Banner, **DNS**, External Authentication, Fragment Settings, HTTP, ICMP, Secure Shell, SMTP Server, SNMP, SSL, Syslog, Timeouts, Time Synchronization, and UCAPL/CC Compliance. The main content area is titled 'DNS Resolution Settings' and includes the instruction 'Specify DNS servers group and device interfaces to reach them.' It features a checked checkbox 'Enable DNS name resolution by device'. Below this are two input fields: 'DNS Server Group*' set to 'Cisco' and 'Expiry Entry Timer' set to '1' (with a range of 1-65535 minutes). Another input field shows 'Poll Timer' set to '240' (with a range of 1-65535 minutes). A section titled 'Interface Objects' explains that devices will use specified interface objects for connecting with DNS Servers. It contains two panels: 'Available Interface Objects' with a search bar and a list of objects (ftd-mgmt, inside, inside-nat, labs, outside, outside-nat, postgrad, privileged, research, servers, servers-nat, staff), and 'Selected Interface Objects' which currently lists 'outside' and 'servers'. An 'Add' button is positioned between the two panels. At the bottom, there is a checked checkbox 'Enable DNS Lookup via diagnostic interface also.'

The screenshot shows the 'Configure DNS' page in the FirePOWER Threat Defense GUI. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device'. The left sidebar shows 'System Settings' with sub-items: Management Access, Logging Settings, DHCP Server, **DNS Server**, Management Interface, Hostname, NTP, and Cloud Services. Below that are 'Traffic Settings' and 'URL Filtering Preferences'. The main content area is titled 'Device Summary' and 'Configure DNS'. It is divided into two main sections: 'Data Interface' and 'Management Interface'. The 'Data Interface' section includes an 'Interfaces' list with a '+' button and 'ANY' selected, a 'DNS Group' dropdown set to 'CiscoUmbrellaDNSServerGroup', and 'FQDN DNS SETTINGS' with 'Poll Time' set to '240' and 'Expiry' set to '1' (both in minutes). A 'SAVE' button is at the bottom. The 'Management Interface' section has a 'DNS Group' dropdown with a filter, showing options 'None', 'CiscoUmbrellaDNSServerGroup', and 'CustomDNSServerGroup' (which is highlighted). A 'Create DNS Group' link is also visible.

Add DNS Group

Name
FQDN-DNS

DNS IP Addresses (up to 6)
10.10.10.10
[Add another DNS IP Address](#)

Domain Search Name

Retries: 2 Timeout: 2

CANCEL OK

Hinweis: Stellen Sie sicher, dass die Systemrichtlinie nach der Konfiguration des DNS auf die FTD angewendet wird. (Der konfigurierte DNS-Server sollte den verwendeten FQDN auflösen.)

Schritt 2: Erstellen Sie dazu das FQDN-Objekt, indem Sie zu **Objekte > Objektverwaltung > Netzwerk hinzufügen > Objekt hinzufügen** navigieren.

Edit Network Object

? X

Name	<input type="text" value="Test-Server"/>
Description	<input type="text" value="Test for FQDN"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input type="radio"/> Network <input checked="" type="radio"/> FQDN
	<input type="text" value="test.cisco.com"/>
	Note: You can use FQDN network objects in access and prefilter rules only
Lookup:	<input type="text" value="Resolve within IPv4 and IPv6"/> ▼
Allow Overrides	<input type="checkbox"/>

Save

Cancel

Dr...

Add Network Object

Name

FQDN

Description

Type

Network Host FQDN

i Note:
You can use FQDN network objects in access rules only.

Domain Name

test.cisco.com

e.g. ad.example.com

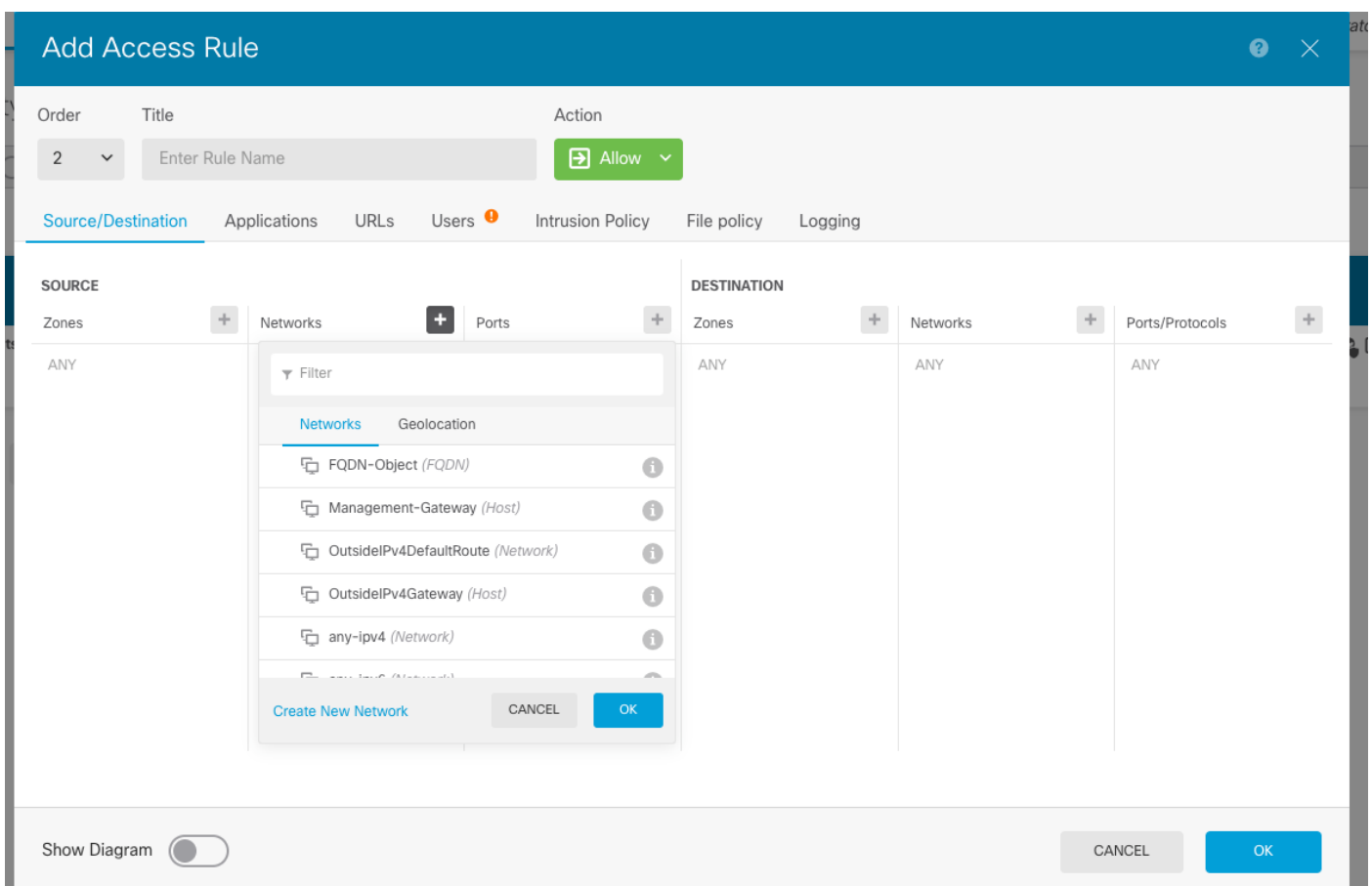
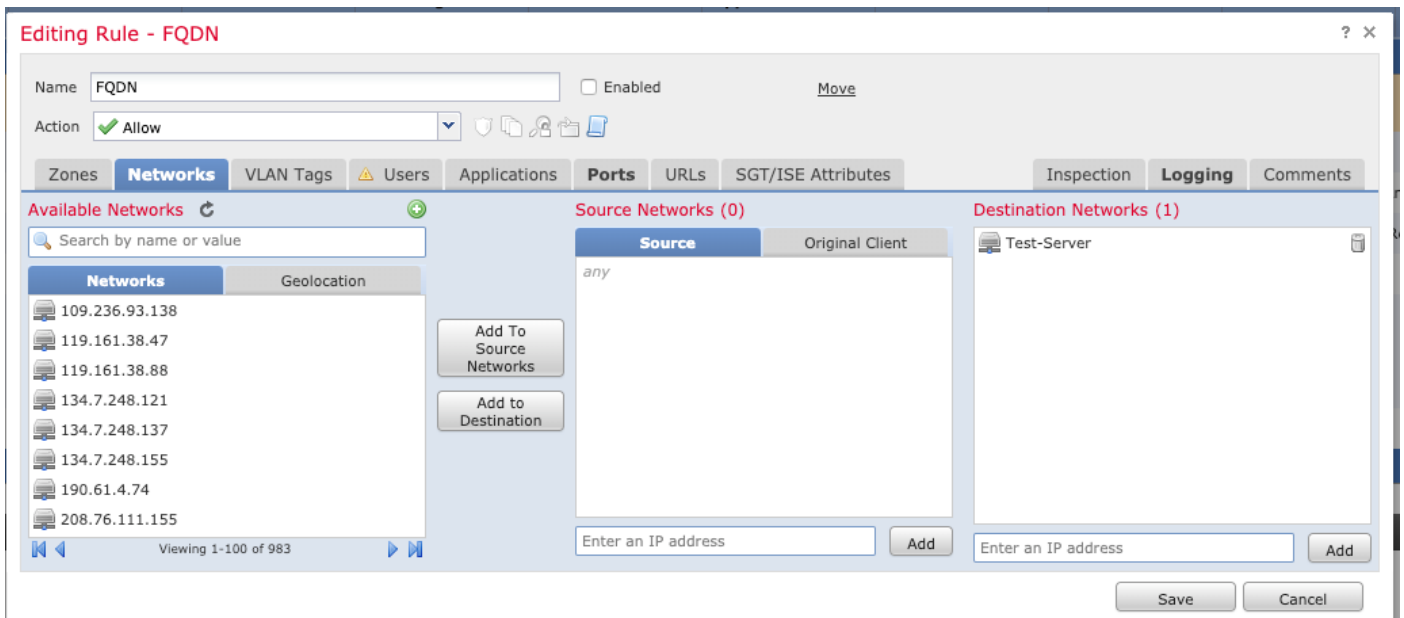
DNS Resolution

IPv4 and IPv6

CANCEL OK

Schritt 3: Erstellen Sie eine Zugriffskontrollregel, indem Sie zu **Richtlinien > Zugriffskontrolle** navigieren.

Hinweis: Sie können eine Regel erstellen oder die vorhandene Regel entsprechend der Anforderung ändern. Das FQDN-Objekt kann entweder in Quell- und/oder Zielnetzwerken verwendet werden.



Stellen Sie sicher, dass die Richtlinie nach Abschluss der Konfiguration angewendet wird.

Überprüfen

Initiieren Sie Datenverkehr vom Client-Computer, der die erstellte FQDN-basierte Regel auslösen soll.

Navigieren Sie im FMC zu **Events > Connection Events (Ereignisse > Verbindungsereignisse)**, und filtern Sie nach dem spezifischen Datenverkehr.

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device	
2019-06-04 16:04:56	2019-06-04 17:05:16	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61132 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1
2019-06-04 16:04:56	2019-06-04 16:04:56	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61132 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1
2019-06-04 12:32:31	2019-06-04 13:32:45	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61115 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1
2019-06-04 12:32:31	2019-06-04 12:32:31	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61115 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1
2019-06-04 12:13:13	2019-06-04 12:13:58	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61097 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1
2019-06-04 12:13:13	2019-06-04 12:13:13	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61097 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1
2019-06-04 12:01:40	2019-06-04 12:01:48	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61066 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1
2019-06-04 12:01:40	2019-06-04 12:01:40	Allow	Intrusion Monitor	21.21.21.101	USA	10.123.175.6		servers	outside	61066 / tcp	22 / ssh / tcp	SSH	SSH client						FTD-1

<< Page 1 of 1 >> Displaying rows 1-8 of 8 rows

View Delete
View All Delete All

Fehlerbehebung

Der DNS-Server sollte in der Lage sein, das FQDN-Objekt aufzulösen. Dies kann über die CLI überprüft werden, die diesen Befehl ausführt:

- Systemunterstützung für Diagnose-CLI
- show fqdn