

Configura oggetto basato su FQDN per la regola di controllo di accesso

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la configurazione dell'oggetto Nome di dominio completo (FQDN) tramite il Centro gestione firewall e viene illustrato come utilizzare l'oggetto FQDN nella creazione delle regole di accesso.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza della tecnologia Firepower.
- Conoscenza della configurazione dei criteri di controllo di accesso in Firesight Management Center (FMC)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower Management Center con versione 6.3 e successive.
- Firepower Threat Defense versione 6.3 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1. Per configurare e utilizzare un oggetto basato su FQDN, configurare innanzitutto

DNS in Firepower Threat Defense.

Accedere al CCP e selezionare **Dispositivi > Impostazioni piattaforma > 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.' There are three main sections: 1. 'Enable DNS name resolution by device' (checked), with 'DNS Server Group*' set to 'Cisco', 'Expiry Entry Timer' set to '1' (range 1-65535 minutes), and 'Poll Timer' set to '240' (range 1-65535 minutes). 2. 'Interface Objects' section with the instruction 'Devices will use specified interface objects for connecting with DNS Servers.' It features two panes: 'Available Interface Objects' (containing a search bar and a list of objects like ftd-mgmt, inside, outside, etc.) and 'Selected Interface Objects' (containing 'outside' and 'servers'). An 'Add' button is between them. 3. 'Enable DNS Lookup via diagnostic interface also.' (checked).

The screenshot shows the 'Configure DNS' configuration page. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device'. The left sidebar has 'System Settings' (with sub-items: Management Access, Logging Settings, DHCP Server, **DNS Server**, Management Interface, Hostname, NTP, Cloud Services) and 'Traffic Settings' (with sub-item: URL Filtering Preferences). The main content area is titled 'Device Summary' and 'Configure DNS'. It is divided into two main sections: 1. 'Data Interface' section with 'Interfaces' set to 'ANY' and 'DNS Group' set to 'CiscoUmbrellaDNSServerGroup'. Below this are 'FQDN DNS SETTINGS' with 'Poll Time' set to '240' minutes and 'Expiry' set to '1' minutes. A 'SAVE' button is at the bottom. 2. 'Management Interface' section with 'DNS Group' set to 'CustomDNSServerGroup'. A dropdown menu is open, showing options: 'None', 'CiscoUmbrellaDNSServerGroup', and 'CustomDNSServerGroup' (which is selected). 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

Nota: Verificare che i criteri di sistema siano applicati all'FTD dopo la configurazione del DNS (il server DNS configurato deve risolvere l'FQDN che verrà utilizzato).

Passaggio 2. Creare l'oggetto FQDN per passare a **Oggetti > Gestione oggetti > Aggiungi rete > Aggiungi oggetto**.

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

Add Network Object

Name
FQDN

Description

Type
 Network Host FQDN

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

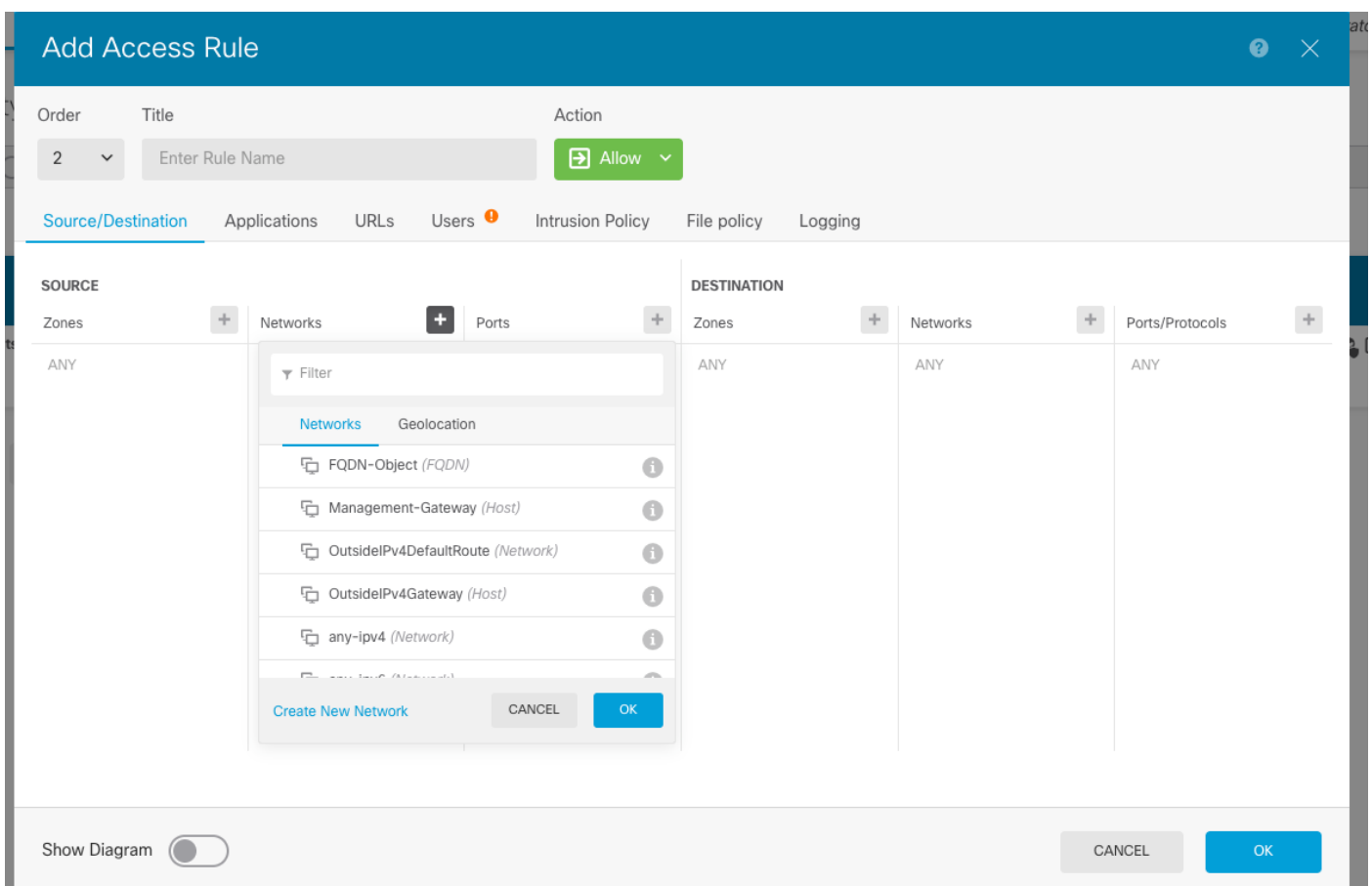
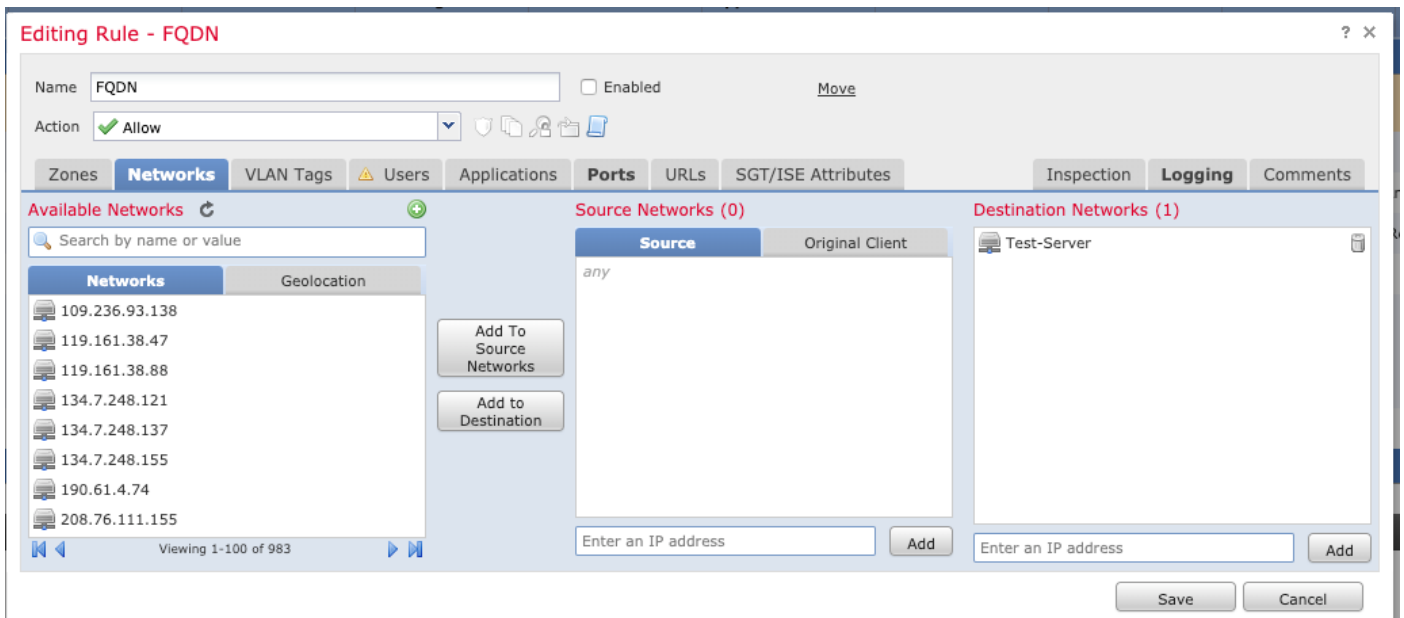
Domain Name
test.cisco.com
e.g. ad.example.com

DNS Resolution
IPv4 and IPv6

CANCEL OK

Passaggio 3. Creare una regola di controllo d'accesso passando a **Criteri > Controllo d'accesso**.

Nota: È possibile creare una regola o modificare la regola esistente in base al requisito. L'oggetto FQDN può essere utilizzato nelle reti di origine e/o di destinazione.



Verificare che il criterio sia applicato dopo il completamento della configurazione.

Verifica

Inizializzare il traffico dal computer client che deve attivare la regola basata su FQDN creata.

Nel FMC, selezionare **Eventi > Eventi di connessione, filtrare per il traffico specifico.**

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

Risoluzione dei problemi

Il server DNS deve essere in grado di risolvere l'oggetto FQDN. È possibile verificare questa condizione dalla CLI che esegue i seguenti comandi:

- `system support diagnostic-cli`
- `mostra fqdn`