Configurer l'objet basé sur FQDN pour la règle de contrôle d'accès

Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Vérification Dépannage

Introduction

Ce document décrit la configuration de l'objet FQDN (Fully Qualified Domain Name) via le Centre de gestion du pare-feu (FMC) et comment utiliser l'objet FQDN dans la création de la règle d'accès.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower.
- Connaissance de la configuration de la stratégie de contrôle d'accès sur Firesight Management Center (FMC)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Management Center exécutant les versions 6.3 et ultérieures.
- Firepower Threat Defense version 6.3 et ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Étape 1. Pour configurer et utiliser un objet basé sur FQDN, commencez par configurer DNS sur Firepower Threat Defense.

Connectez-vous au FMC et accédez à **Devices > Platform Settings > DNS**.

| APP Inspection | DNS Resolution Settin | as | | | | | | | | |
|-------------------------|--------------------------------------|----------------------|-----------------------|-----------------------|--------|--|--|--|--|--|
| Banner | Specify DNS servers grou | n and device inter | faces to reach them | | | | | | | |
| > DNS | opeany bits servers grou | p and derive inter | to reach them | | | | | | | |
| External Authentication | Enable DNS name resolution by device | | | | | | | | | |
| External Authentication | DNS Server Group* | Cisco | | | | | | | | |
| | Divo Server Group*. | CISCO | • | | | | | | | |
| TITP | Evolution Entry Timory | | Dana | au 1 6EE2E minutas | | | | | | |
| ICMP Comme Chall | Expiry Entry Timer: | 1 | Rang | e: 1-65535 minutes | | | | | | |
| Secure Shell | Poll Timer: | 240 | Rang | e: 1-65535 minutes | | | | | | |
| Shine Server | | | | | | | | | | |
| SIMP | Interface Objects | | | | | | | | | |
| Suchan | Devices will use specif | ied interface obje | cts for connecting wi | th DNS Servers. | | | | | | |
| Sysiog | Available Interface (| biects C | | Selected Interface Ob | viects | | | | | |
| Time Sunchronization | Search | | I | | | | | | | |
| | Search | | J | outside | | | | | | |
| UCAPL/CC Compliance | 📩 ftd-mgmt | | | servers | | | | | | |
| | 👬 inside | | | | | | | | | |
| | 📇 inside-nat | | | | | | | | | |
| | alabs | | | | | | | | | |
| | 📇 outside | | Add | | | | | | | |
| | 🖧 outside-nat | | | | | | | | | |
| | 🚠 postgrad | | | | | | | | | |
| | 📩 privileged | | | | | | | | | |
| | research | | | | | | | | | |
| | and servers | | | | | | | | | |
| | servers-nat | | | | | | | | | |
| | staff | | | | | | | | | |
| | and starr | | | | | | | | | |
| | Enable DNS Looku | o via diagnostic int | erface also. | | | | | | | |
| | | | | | | | | | | |

| cisco. | Monitoring Policies O | ₩. bjects | Device | | | | <u>></u> | | 9 | ? | admin Administrator | • |
|--|--------------------------------------|--------------|---------------|---------|---------------------|-------------------|-------------|---|---|---|------------------------|---|
| System Settings ← Management Access | Device Summary Configure DNS | | | | | | | | | | | |
| Logging Settings | Data Interface | | | | Management Int | terface | | | | | | |
| DHCP Server | Interfaces + | | | | DNS Group Filter | | | | | | | ~ |
| Management Interface Hostname | ANY | | | | None | llaDNSServerGroup | | 0 | | | | |
| NTP | DNS Group CiscoUmbrellaDNSServerG | iroup | | ~ | CustomDNSS | ServerGroup | | 0 | | | | |
| Cloud Services | FQDN DNS SETTINGS | | | | Create DNS Group | | | | | | | |
| URL Filtering Preferences | Poll Time 240 | minute | Expiry s 1 | minutes | | | | | | | | |
| | 1 - 65535 SAVE | | 1 - 65535 | | | | | | | | | |

| Add DNS (| Group | | 0 | × |
|--------------------|-------------|--------|----|---|
| Name | | | | |
| FQDN-DNS | | | | |
| DNS IP Addresse | s (up to 6) | | | |
| 10.10.10.10 | | | | |
| Add another DNS IP | Address | | | |
| Domain Search N | ame | | | |
| Retries | Timeout | | | |
| 2 | 2 | | | |
| | | | _ | |
| | | CANCEL | ОК | |
| 535 | | | | |

Note: Assurez-vous que la stratégie système est appliquée au FTD après avoir configuré le DNS. (Le serveur DNS configuré doit résoudre le nom de domaine complet qui sera utilisé)

Étape 2. Créez l'objet FQDN, afin de faire cela naviguez jusqu'à **Objets > Gestion des objets > Ajouter un réseau > Ajouter un objet.**

| Edit Network | Object | | | | ? × |
|-----------------|---------------------|------------------|----------|------|--------|
| Name | Test-Server | | | | |
| Description | Test for FQDN | I | | | |
| Network | 🔿 Host | 🔘 Range | ONetwork | FQDN | |
| | test.cisco.com | 1 | | | |
| | Note: You can us | ilter rules only | | | |
| Lookup: | Resolve within | n IPv4 and IPv6 | | ~ | |
| Allow Overrides | | | | | |
| | | | | Save | Cancel |
| | | | | | |
| | | | | | |

Add Network Object

D

| Name | | | | |
|-----------------------|----------------|------------------|----------------|----|
| FQDN | | | | |
| Description | | | | |
| | | | | 1, |
| Туре | | | | |
| O Network | ◯ Host | 🔘 FQDN | | |
| i Note: You can us | e FQDN network | objects in acces | ss rules only. | |
| Domain Name | | | | |
| test.cisco.com | | | | |
| e.g. ad.example.cor | n | | | |
| DNS Resolution | | | | |
| IPv4 and IPv6 | | ~ | | |
| | | | | |
| | | | CANCEL | ОК |
| | | | | |
| | | | | |

0

 \times

Étape 3. Créez une règle de contrôle d'accès en accédant à **Politiques > Contrôle d'accès**.

Note: Vous pouvez créer une règle ou modifier la règle existante en fonction de la condition requise. L'objet FQDN peut être utilisé dans les réseaux source et/ou de destination.

| Editing Rule - FQDN | | | | ? × |
|----------------------------------|--------------------|-------------------------|----------------------|------------------|
| Name FQDN | 🗌 Enab | led <u>Move</u> | | |
| Action Allow | 🔹 U D 2 🗠 🗖 | | | |
| Zones Networks VLAN Tags 🛆 Users | Applications Ports | URLs SGT/ISE Attributes | Inspection | Logging Comments |
| Available Networks 🖒 📀 | Source | Networks (0) | Destination Networks | (1) |
| Search by name or value | | Source Original Clier | nt 📄 Test-Server | ĩ |
| Networks Geolocation | any | | | |
| 109.236.93.138 | | | | |
| 119.161.38.47 | Add To Source | | | |
| 119.161.38.88 | Networks | | | |
| 134.7.248.121 | Add to | | | |
| 134.7.248.137 | Destination | | | |
| 134.7.248.155 | | | | |
| 190.61.4.74 | | | | |
| 208.76.111.155 | Entern | ID address | | |
| Viewing 1-100 of 983 | enter al | | Enter an IP address | Add |
| | | | | Save Cancel |

| Add Access Rule | e | | | | | 8 × | ä | | | |
|------------------------|---|------------|------------------|------------|-----------------|-----|---|--|--|--|
| Order Title | Action | Action | | | | | | | | |
| 2 🗸 Enter Rule N | lame 🔁 All | Allow Y | | | | | | | | |
| Source/Destination App | olications URLs Users ⁹ Intrusion Po | olicy File | e policy Logging | | | | | | | |
| SOURCE | | DE | STINATION | | | | | | | |
| Zones + | Networks Ports | + Zor | + | Networks + | Ports/Protocols | + | | | | |
| ANY | ▼ Filter | A | NY | ANY | ANY | | | | | |
| | Networks Geolocation | | | | | | ł | | | |
| | FQDN-Object (FQDN) | 0 | | | | | | | | |
| | G Management-Gateway (Host) | 0 | | | | | | | | |
| | CutsidelPv4DefaultRoute (Network) | 0 | | | | | | | | |
| | CutsidelPv4Gateway (Host) | 0 | | | | | | | | |
| | any-ipv4 (Network) | 0 | | | | | | | | |
| | En and land (Alational) | | | | | | | | | |
| | Create New Network CANCEL | OK | | | | | | | | |
| | | | | | | | | | | |
| Show Diagram | | | | C | ANCEL | ОК | | | | |

Assurez-vous que la stratégie est appliquée une fois la configuration terminée.

Vérification

Lancez le trafic à partir de la machine cliente qui devrait déclencher la règle basée sur FQDN créée.

Sur le FMC, accédez à **Events > Connection Events, filtrez le trafic spécifique.**

| • | | | | | | | | | | | | | | | | | | | | |
|--------------------------|--------|---------------------|-------------------------|--------|-------------------|----------------------|----------------------|---------------------|----------------------|--------------------------|-------------------------|----------------------------|---------------------------------|-------------------------|------------|--------------------|-----|-----------------|-------------------|--------|
| | | ★ 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 |
| 4 | | 2019-06-04 16:04:56 | 2019-06-04 17:05:16 | Allow | Intrusion Monitor | 21.21.21.101 | SA USA | 10.123.175.6 | | servers | outside | 61132 / tcp | 22 (ssh) / tcp | SSH | SSH client | | | | | FTD-1 |
| 4 | | 2019-05-04 16:04:56 | | Allow | Intrusion Monitor | 21.21.21.101 | usa 🔜 | <u>10.123.175.6</u> | | servers | outside | 61132 / tcp | 22 (ssh) / tcp | SSH | SSH client | | | | | FTD-1 |
| 4 | | 2019-05-04 12:32:31 | 2019-06-04 13:32:45 | Allow | | 21.21.21.101 | usa 🛄 | 10.123.175.6 | | servers | outside | 61115 / tcp | 22 (ssh) / tcp | SSH | SSH client | | | | | FTD-1 |
| 4 | | 2019-06-04 12:32:31 | | Allow | | 21.21.21.101 | SA USA | 10.123.175.6 | | servers | outside | 61115 / tcp | 22 (ssh) / tcp | | | | | | | FTD-1 |
| 4 | | 2019-06-04 12:13:13 | 2019-06-04 12:13:54 | Allow | Intrusion Monitor | 21.21.21.101 | USA USA | 10.123.175.6 | | servers | outside | 61097 / tcp | 22.(ssh)./.tcp | SSH | SSH client | | | | | FTD-1 |
| 4 | | 2019-05-04 12:13:13 | | Allow | Intrusion Monitor | 21.21.21.101 | usa usa | 10.123.175.6 | | servers | outside | 61097 / tcp | 22 (ssh) / tcp | SSH | SSH client | | | | | FTD-1 |
| 4 | | 2019-06-04 12:01:40 | 2019-06-04 12:01:48 | Allow | Intrusion Monitor | 21.21.21.101 | SA USA | 10.123.175.6 | | servers | outside | 61066 / tcp | 22 (ssh) / tcp | SSH | SSH client | | | | | FTD-1 |
| 4 | | 2019-06-04 12:01:40 | | Allow | Intrusion Monitor | <u> 21.21.21.101</u> | SA USA | 10.123.175.6 | | servers | outside | 61066 / tcp | 22 (ssh) / tcp | SSH | SSH client | | | | | FTD-1 |
| $ \langle \cdot \rangle$ | < Page | 1 of 1 >> Displa | ying rows 1-8 of 8 rows | | | | | | | | | | | | | | | | | |
| | View | Delete | | | | | | | | | | | | | | | | | | |
| | View A | II Delete All | | | | | | | | | | | | | | | | | | |

Dépannage

Le serveur DNS doit être en mesure de résoudre l'objet FQDN, ceci peut être vérifié à partir de l'interface de ligne de commande exécute la commande suivante :

- support système diagnostic-cli
- show fqdn

.