Verify OSPF MD5 Authentication Config on FTD

Contents

- Issue
- Environment
- Resolution
- Cause
- Related Content

Issue

Open Shortest Path First (OSPF) adjacency failures occur between an adjacent device and a Cisco Secure Firewall Threat Defense (FTD) due to authentication mismatch errors. The OSPF sessions fail specifically with OSPF Message-Digest Algorithm 5 (MD5) authentication mismatches. During troubleshooting, you must verify that the OSPF MD5 authentication key in the FTD matches the key configured on the adjacent device.

<#root>

```
firepower# debug ip ospf adjacency
OSPF adjacency events debugging is on
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1

OSPF: Rcv pkt from 10.X.X.9, OT-Zone2 : Mismatch Authentication type. Input packet specified type 2, we
OSPF: Rcv pkt from 10.X.X.1, OT-Zone : Mismatch Authentication type. Input packet specified type 2, we u
OSPF: Rcv pkt from 10.X.X.9 : Mismatched Authentication key - ID 1
OSPF: Rcv pkt from 10.X.X.1 : Mismatched Authentication key - ID 1


OSPF: Send with youngest Key 1

OSPF: Rcv pkt from 10.X.X.9, OT-Zone2 : Mismatch Authentication type. Input packet specified type 2, we


OSPF: Send with youngest Key 1

OSPF: Rcv pkt from 10.X.X.9 : Mismatched Authentication key - ID 1
```

```
OSPF: Rcv pkt from 10.X.X.1, OT-Zone : Mismatch Authentication type. Input packet specified type 2, we u
OSPF: Rcv pkt from 10.X.X.1 : Mismatched Authentication key - ID 1
```

Environment

- Cisco Secure Firewall Firepower managed by Firewall Management Center (FMC) (all versions)
- Adjacent network device OSPF connection by MD5 authentication

Resolution

1.- Execute these command to display the OSPF MD5 authentication configuration. This command displays the OSPF MD5 authentication settings applied to the interfaces.

<#root>

```
firepower#
```

```
more system:running-config | inc md5
```

2.- Use the preceding output to compare the MD5 authentication key configuration between the FTD and adjacent devices.

3.- Navigate to **Devices > Device Management > Edit Device > Routing > OSPF > Interface > Authentication**. Update the MD5 authentication key in order to match the configuration on the adjacent side, then deploy the policy to the FTD. Otherwise, configure the adjacent device in order to match the FTD MD5.

Note: OSPF MD5 keys are not retrievable in plaintext on Cisco platforms for security reasons. The verification method described in this section shows the effective configuration but does not expose the actual key values in plaintext format.

Cause

OSPF adjacency failed due to a mismatch in the OSPF MD5 authentication key between the adjacent Cisco network device and the FTD interface configuration. While the key could not be viewed in plaintext by design, verification on the FTD confirmed the effective MD5 configuration, allowing identification and reconciliation of the mismatch.

Related Content

- Troubleshoot OSPF Configuration in FTD
- Cisco Secure Firewall Configuration Guides
- Cisco Technical Support & Downloads