Recommendations Against Password Spray Attacks Aimed at Remote Access VPN Services in Secure Firewall

Contents

Introduction

This document describes recommendations to consider against password-spray attacks aimed at Remote Access VPN services in Secure Firewall.

Background Information

Password spray attacks are a type of brute-force attack where an attacker attempts to gain unauthorized access to multiple user accounts by systematically trying a few commonly used passwords across many accounts. Successful password spray attacks can lead to unauthorized access to sensitive information, data breaches, and potential compromises of network integrity

Moreover, these attacks, even when unsuccessful in their attempt to gain access, can consume computational resources from the Secure Firewall and prevent valid users from connecting to the remote access VPN services.

Observed Behaviors

When your Secure Firewall is targeted by password-spray attacks in Remote Access VPN services, you can identify these attacks by monitoring syslogs and using specific show commands. The most common behaviors to look for include:

Unusual Amount of Rejected Authentication Requests

The VPN headend Cisco Secure Firewall ASA or FTD shows symptoms of password-spray attacks with an unusual rate (100-thousands or millions) of rejected authentication attempts.

Note: These unusual attempts to authenticate can be directed towards either the LOCAL database or external authentication servers.

The best way to detect this is by looking at the syslog. Look for an unusual number of any of the next ASA syslog IDs:

- %ASA-6-113015

<#root>

```
%ASA-6-113015
: AAA user authentication Rejected : reason = User was not found : local database :
user
 = admin : user
IP
 = x.x.x.x
```

- %ASA-6-113005

<#root>

```
%ASA-6-113005
: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =
```

- %ASA-6-716039

<#root>

```
%ASA-6-716039
: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.
```

The username is always hidden until the **no logging hide username** command is configured on the ASA.

> **Note**: This gives insight into verifying if valid users are generated or known by offending IPs however, please be cautious as usernames will be visible in the logs.

To verify, log in to the ASA or FTD Command Line Interface (CLI), run the **show aaa-server** command, and investigate for an unusual number of attempted and rejected authentication requests to any of the configured AAA servers:

<#root>

```
ciscoasa# show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against external server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms

Number of authentication requests 2228536 - - - - - >>>> Unusual increments


Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312

Number of rejects 2225363 - - - - - >>>> Unusual increments / Unusual rejection rate


Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

Recommendations

Consider and apply the next recommendations.

1. Enable Logging.

Logging is a crucial part of cybersecurity that involves recording events happening within a system. The absence of detailed logs leaves gaps in understanding, hindering a clear analysis of the attack method. It is recommended that you enable logging to a remote syslog server for improved correlation and auditing of network and security incidents across various network devices.

For information on how to configure logging, see the next platform-specific guides:

Cisco ASA Software:

- Use Guide to Secure ASA Firewall
- Logging chapter of the Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide

Cisco FTD Software:

- Configure Logging on FTD via Firewall Management Center (FMC)
- Configure Syslog section in the Platform Settings chapter of the Cisco Secure Firewall Management Center Device Configuration Guide
- Configure and Verify Syslog in Firepower Device Manager
- Configuring System Logging Settings section in the System Settings chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager

Note: The syslog message IDs necessary to verify the behaviors outlined in this document (113015, 113005 & 716039), must be enabled at the **informational level (6)**. These IDs fall within the 'auth' and 'webvpn' logging classes.

2. Configure Threat Detection Features or Hardening Measures for Remote Access VPN.

To help mitigate the impact and reduce the likelihood of occurrence of these brute-force attacks on your RAVPN connections, you can review and apply the next configuration options:

Option 1 (preferred): Configure Threat Detection for Remote Access VPN Services.

Threat detection features for remote access VPN services allow you to protect against these kind of attacks by automatically blocking the host (IP address) that exceeds the configured thresholds, to prevent further attempts until you manually remove the shun of the IP address.

These threat detection features are currently supported in the Cisco Secure Firewall versions listed next:

ASA Software:

- **9.16 version train** -> supported from 9.16(4)67 and newer versions within this specific train.
- **9.18 version train** -> supported from 9.18(4)40 and newer versions within this specific train.
- **9.20 version train** -> supported from 9.20(3) and newer versions within this specific train.
- **9.22 version train** -> supported from 9.22(1.1) and any newer versions.

FTD Software:

- **7.0 version train** -> supported from 7.0.6.3 and newer versions within this specific train.
- **7.6 version train** -> supported from 7.6.0 and any newer versions.

Note: These features are currently **not supported in version trains 7.1, 7.2, 7.3, or 7.4**. This document is updated as they become available.

For full details and configuration guidance, please refer to the next documents:

- Configuration on Secure Firewall ASA: Configure Threat Detection for Remote Access VPN on Secure Firewall ASA.
- Configuration on Secure Firewall FTD: Configure Threat Detection for Remote Access VPN Services on Secure Firewall Threat Defense

Option 2: Apply Hardening Measures for Remote Access VPN.

If the threat detection features for Remote Access VPN services are not supported in your Secure Firewall version, implement all the next hardening measures to mitigate the impact of these attacks:

1. Disable AAA Authentication in the DefaultWEBVPN and DefaultRAGroup Connection Profiles (step-by-step: ASA | FTD managed by FMC).
2. Disable Secure Firewall Posture (Hostscan) from the DefaultWEBVPNGroup and DefaultRAGroup (step-by-step: ASA | FTD managed by FMC).
3. Disable Group-aliases and Enable Group-URLs in the rest of the connection profiles (step-by-step: ASA | FTD managed by FMC).

Note: If you require support with FTD managed through local Firewall Device Management (FDM), please contact the Technical Assistance Center (TAC) for expert guidance.

For further details please refer to the Implement Hardening Measures for Secure Client AnyConnect VPN guide.

Option 3: Manually Block Connection Attempts from Malicious Sources.

In order to impede connection attempts from unauthorized sources, you can implement any of the options listed below:

- Use the "shun" command:

This is a straightforward approach to blocking a malicious IP, however, it must be done manually. Please read the section Alternative configuration to block attacks for secure firewall using the 'shun' Command for further details.

- Configure Control-plane ACL:

Implement a control-plane ACL on the ASA/FTD to filter out unauthorized public IP addresses and prevent them from initiating remote VPN sessions. Configure Control Plane Access Control Policies for Secure Firewall Threat Defense and ASA.

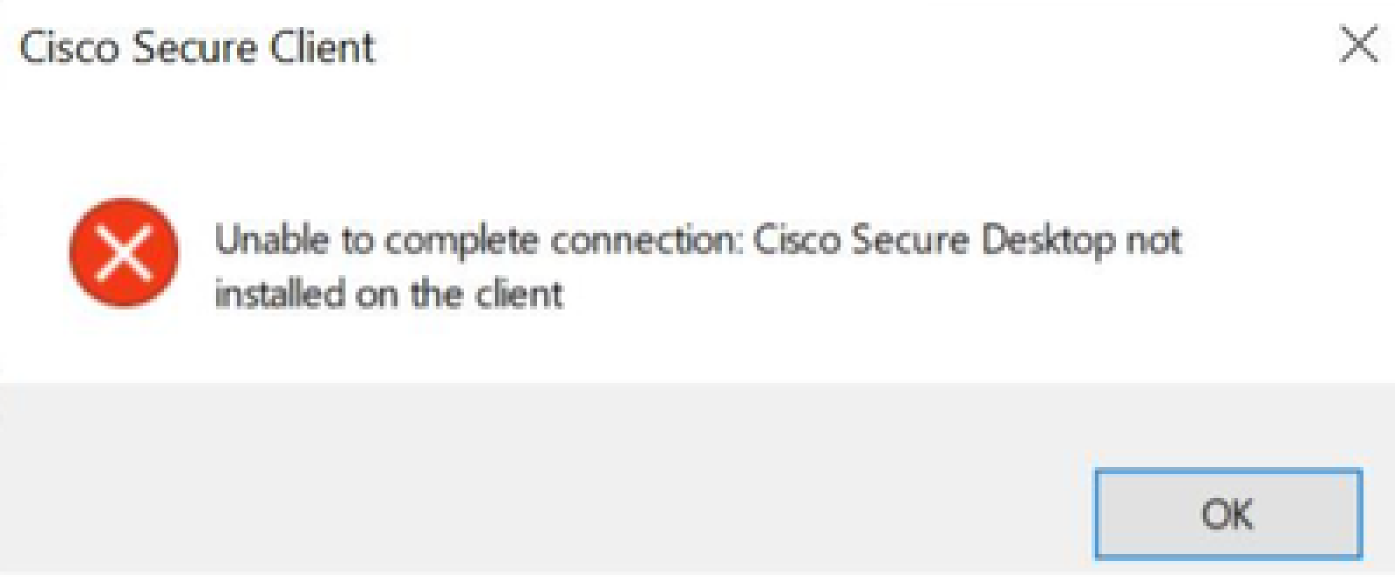
Note: Cisco Talos has published a list of IP addresses and credentials associated with these attacks. A link to their GitHub repository can be found in the "IOCs" section of their advisory. It is important to note that the source IP addresses for this traffic are likely to change, therefore, you must review the security logs (syslog) to identify the problematic IP addresses. Upon identification, any of the 3 options can be used to block them.

Related Behaviors

There are certain symptoms that can be experienced as a consequence of the Secure Firewall being targeted by password spray attacks. To resolve these issues, consider implementing the recommendations provided in this document.

Side Symptom 1: Unable to establish VPN connections with Cisco Secure Client (AnyConnect) when Firewall Posture (HostScan) is enabled

When attempting to establish a RAVPN connection using Cisco Secure Client (AnyConnect), users can intermittently encounter an error message that states, **"Unable to complete connection. Cisco Secure Desktop not installed on the client."**. This behavior typically arises when there is a failure to allocate a hostscan token by the VPN headend, either a Cisco Secure Firewall ASA or FTD. Notably, this allocation failure correlates with instances of brute-force attacks targeting the Secure Firewall infrastructure and prevents the successful completion of the VPN connection process.. This behavior was tracked and resolved via Cisco bug ID CSCwj45822.



Unable to complete connection: Cisco Secure Desktop not installed on the client

Note: This specific behavior occurs only when Firewall Posture (HostScan) is enabled at the headend, regardless of the Secure Client or AnyConnect version used.

To confirm if the VPN headend Cisco Secure Firewall ASA or FTD show symptoms of hostscan token allocation failures, run the **debug menu webvpn 187 0** command.

```
<#root>

ASA# debug menu webvpn 187 0
Allocated Hostscan token = 1000

Hostscan token allocate failure = xxx - - - - > Increments
```

Note: The occurrence of this issue is a consequence of the attacks. This behavior was tracked and resolved via Cisco bug ID CSCwj45822.

To resolve this issue, consider implementing the recommendations provided in this document.

Additional Hardening Implementations for RAVPN

You can consider additional countermeasures that require extra changes to your deployments to harden the security of your Remote Access VPN deployment, such as adopting **certificate-based authentication** for RAVPN. Please refer to the Implement Hardening Measures for Secure Client AnyConnect VPN document for detailed configuration guidance.

Additional Information

- Cisco ASA Forensic Investigation Procedures for First Responders
- Cisco Firepower Threat Defense Forensic Investigation Procedures for First Responders
- Cisco Talos Threat Advisory
- For additional assistance, please contact the Technical Assistance Center (TAC). A valid support contract is required: Cisco Worldwide Support Contacts.