ADMIN HANDBUCH

GFI LanGuard KI WAN-Agent-Funktion

GFI Software™

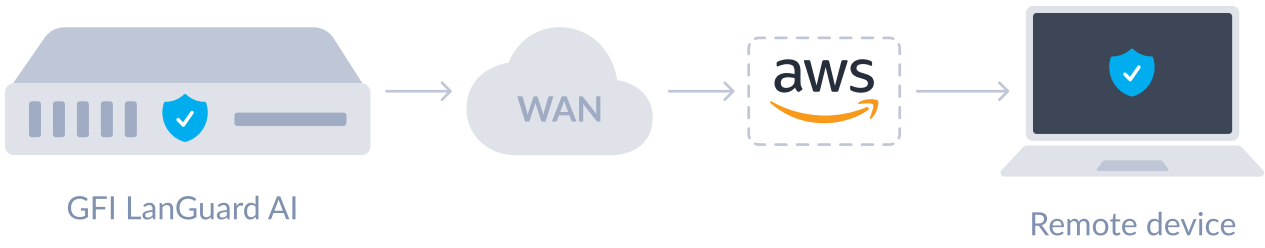
Letztes Änderungsdatum: 26.12.2024

GFI LanGuard KI's WAN-Agent

Der WAN-Agent ist eine neue Funktion, die Kunden hilft, entfernte Benutzer ohne VPN zu scannen. Er ermöglicht es den Kunden, Schwachstellen in verteilten Infrastrukturen von einer zentralen Schnittstelle aus zu identifizieren und zu beheben. Mit seinem leichten Design und minimalen Ressourcenverbrauch sorgt der WAN-Agent für eine optimale Ressourcennutzung, sodass Sie Ihre Strategie zur Schwachstellenbewertung und Patch-Verwaltung optimieren können.

Wie funktioniert es?

Der WAN-Agent wird auf jedem entfernten Computer installiert, der aus der LanGuard-Konsole heraus gescannt und gepatcht werden muss.



Der WAN-Agent und die LanGuard-Konsole kommunizieren sicher über AWS, um Befehle zum Scannen und Patchen zu senden/zu empfangen. Die vom WAN-Agent verwendeten Ports sind 443, 8443 und 8883.

Aktivierung der WAN-Agent-Funktion

Voraussetzungen

Sie benötigen die folgenden Informationen, um den WAN-Agent zu nutzen. Wenn Sie bereits eine bestehende LanGuard-Installation haben, wenden Sie sich bitte an den Kundenservice, um die benötigten Informationen zu erhalten.
Mandanteninformationen:

- Zertifikat zur Bereitstellung (Datei): unternehmensname_zert.pem
- Privater Schlüssel für das Zertifikat (Datei): unternehmens_private_key.pem
- Zertifikat-ID (Zeichenfolge): 1aaf76we24ff9933g5509q34q347d2h4sg528249dd3e5745f0d13b6513b4115d
- Mandanten-ID (Zeichenfolge): unternehmensname
- GFI LanGuard KI-Server WAN-Name (Zeichenfolge): unternehmensname-8182e550-7186-4cf7-8156-1a5a7f09f123
- GFI LanGuard KI-Serverzertifikat (Datei): unternehmensname-8182e550-7186-4cf7-8156-1a5a7f09f123_zert.pem
- GFI LanGuard KI-Server privater Schlüssel (Datei): unternehmensname-8182e550-7186-4cf7-8156-1a5a7f09f123_private_key.pem

Hinweis: Die obigen Werte sind nur Beispielwerte. Sie sind nicht für die Konfiguration der WAN-Agent-Funktion gedacht.

Die ausgehende Kommunikation sollte von den Ports 443, 8443 und 8883 auf den Zielmaschinen, auf denen der WAN-Agent installiert ist, erlaubt sein.

Serverinstallation / Upgrade

1. Laden Sie das Microsoft Visual C++ Redistributable auf dem Server herunter, auf dem LanGuard installiert ist oder installiert werden soll. Wenn der Installer Ihnen mitteilt, dass die erforderliche Version bereits auf dem Computer installiert ist, können Sie diesen Schritt überspringen.
2. Installieren oder aktualisieren Sie GFI LanGuard KI auf die Version, die die WAN-Funktion unterstützt.

Aktivierung der WAN-Agent-Funktionalität auf dem Server

1. Öffnen Sie die GFI LanGuard KI-Konsole und gehen Sie zu Konfiguration > Agentenverwaltung > WAN-Agenteneinstellungen.
2. In den 6 Eingabefeldern des Dialogs geben Sie die Mandanteninformationen und die von GFI bereitgestellten Dateien an.
3. Sie können die Offline-Zeitüberschreitung des WAN-Agenten (in Stunden) konfigurieren, die definiert, wie lange die LanGuard-Konsole auf einen WAN-Agenten wartet, bevor er als inaktiv betrachtet und von dem Zielcomputer entfernt wird. "Offline" bedeutet, dass es keine Kommunikation zwischen dem WAN-Agenten und der LanGuard-Konsole gegeben hat, was auftreten kann, wenn der Zielcomputer keinen Internetzugang hat oder außer Betrieb genommen wurde.
4. Sie können auch die Bandbreite begrenzen, die die WAN-Agenten beim Herunterladen von Patches verwenden, indem Sie "Download-Bandbreitenlimit aktivieren" auswählen und die gewünschte MB/s-Einstellung vornehmen.
5. Sobald Sie alle Details ausgefüllt haben, klicken Sie auf "WAN-Agent-Installer generieren", um die MSI-Datei des WAN-Agenten-Installers zu erstellen. Notieren Sie sich den Speicherort der generierten Dateien. (Es dauert einige Sekunden, um die Installationsdatei zu generieren).
6. Klicken Sie abschließend auf Übernehmen.

Agenteninstallation

Befolgen Sie diese Schritte, um den Agenten auf den Zielmaschinen zu installieren, die von LanGuard aus der Ferne gescannt und gepatcht werden sollen:

1. Laden Sie das Microsoft Visual C++ Redistributable herunter und installieren Sie es. Wenn der Installer Ihnen mitteilt, dass die erforderliche Version bereits auf dem Computer installiert ist, können Sie diesen Schritt überspringen.
2. Wenn Sie zuvor GFI LanGuard KI-Agenten ausgeführt haben, können Sie den Befehl "MsiExec.exe /X{160301DE-306A-4ADE-8A47-BC5790AF0486}" ausführen, um vorherige Installationen zu deinstallieren.
3. Laden Sie die LanGuardWANAgent.msi herunter, die im Schritt 5 der Aktivierung der WAN-Agent-Funktion erstellt wurde, klicken Sie mit der rechten Maustaste darauf und führen Sie sie als Administrator auf dem Remote-Computer aus:
    - Wenn Sie es ohne Administratorrechte installieren, müssen Sie den Agenten nach der Installation manuell starten (dies muss nur einmal erfolgen). Sie können dies überprüfen, indem Sie "services.msc" in der Eingabeaufforderung ausführen und nach dem Dienst mit dem Namen "GFI LanGuard 12 Attendant Service" suchen.
4. Sobald die Installation abgeschlossen ist und die Verbindung erfolgreich hergestellt wurde, wird ein neuer Knoten für diesen Agenten unter "Remote-Geräte" im Computerbaum des GFI LanGuard KI-Server-Dashboards angezeigt, mit dem Namen des Zielcomputers.

Wichtig: Wenn der Installer abgeschlossen ist, überprüfen Sie bitte unter Dienste, ob der GFI Attendant-Dienst läuft.

Führen Sie einen Scan durch

Sobald der Agent installiert ist, wird er automatisch in der LanGuard-Konsole unter "Remote-Geräte" angezeigt. Um einen Scan zu starten, wählen Sie den neu hinzugefügten Computer aus und folgen Sie den nächsten Schritten:

1. Klicken Sie mit der rechten Maustaste auf den Computer und gehen Sie zu Scan > Benutzerdefinierter Scan. Alternativ können Sie eine Gruppe von Computern auswählen, auf denen der Agent bereitgestellt wurde.
2. Wählen Sie das Scan-Profil aus, das verwendet werden soll, um Informationen zu sammeln.
3. Klicken Sie auf "Scan".
4. Der Scan wird gestartet, aber es werden keine Eingaben in der Konsole empfangen, da der Scan direkt auf dem Zielcomputer ausgeführt wird.

Überwachen Sie den Scan-Vorgang

Um den Scan-Vorgang zu überwachen, können Sie zu Aktivitätsmonitor > Sicherheits-Scans gehen.

Anhang

WAN-Agent-Kommunikationsprotokolle

Für die WAN-Agent-Funktion werden Nachrichten zwischen den WAN-Agenten und der LanGuard-Konsole ausgetauscht. Diese Nachrichten werden in mehrere verschiedene Kategorien eingeteilt:

- 1XX (Agent zu Server): Dies sind spezifische, gezielte Nachrichten, die vom Agenten initiiert werden, um seinen Status zu kommunizieren, Aktionen wie das Ändern von Netzwerkmodi (WAN/LAN), das Initiieren von Scans oder das Senden von Updates durchzuführen. Beispiele sind:
  - AgentInstalled (100): Benachrichtigt den Server, dass ein Agent installiert wurde.
  - AgentSwitchToWAN (101): Informiert den Server, dass der Agent in den WAN-Modus wechselt.
  - AgentScanStart (110): Der Agent informiert den Server, dass er einen Scan gestartet hat.
- 2XX (Broadcast durch Agent): Broadcast-Nachrichten, die von Agenten initiiert werden.
- 3XX (Agentenbestätigungen): Dies sind Bestätigungsnachrichten (ACK), die von Agenten gesendet werden, um den Erhalt oder die erfolgreiche Ausführung von Anfragen, die vom Server initiiert wurden, zu bestätigen. Zum Beispiel:
  - AgentScanRequest_ACK (300): Bestätigt die Scananforderung des Servers.
  - AgentUpdateRequest_ACK (303): Bestätigt die Anfrage des Servers zur Aktualisierung des Agenten.
- 4XX (Agentenfehlermeldungen): Diese Nachrichten zeigen Fehler an, die während von Agenten initiierten Aktionen aufgetreten sind. Beispiele sind:
  - AgentDeployPatchAgentRequest_ERR (401): Zeigt an, dass ein Fehler aufgetreten ist, während der Agent versuchte, einen Patch bereitzustellen.
  - AgentUpdateRequest_ERR (403): Signalisiert ein Problem mit dem Aktualisierungsprozess des Agenten.

- 5XX (Server zu Agentenanforderungen): Dies sind direkte Nachrichten vom Server an den Agenten, die spezifische Aktionen anfordern. Zum Beispiel:
  - ServerRequestScan (500): Fordert den Agenten auf, einen Scan zu starten.
  - ServerRequestDeployPatchAgent (501): Fordert den Agenten auf, einen Patch bereitzustellen.
- 6XX (Broadcast durch Server): Dies wären Broadcast-Nachrichten, die vom Server initiiert werden.
- 7XX (Serverbestätigungen): Dies sind Bestätigungsnachrichten, die vom Server als Antwort auf Agentenaktionen gesendet werden. Zum Beispiel:
  - ServerAgentInstalled_ACK (700): Bestätigt, dass der Server die Agenteninstallation anerkennt.
  - ServerScanStart_ACK (710): Bestätigt die Benachrichtigung des Agenten über den Scanstart.
- 8XX (Serverfehlermeldungen): Diese Nachrichten zeigen Fehler an, die während serverinitiierter Aktionen oder als Antwort auf Agentenaktionen aufgetreten sind. Zum Beispiel:
  - ServerAgentInstalled_ERR (800): Zeigt ein Problem mit der Handhabung der Agenteninstallation durch den Server an.
  - ServerScanFinished_ERR (812): Zeigt an, dass ein Fehler aufgetreten ist, als der Scan abgeschlossen wurde.

Zusammenfassend lässt sich sagen, dass das System ein strukturiertes Kommunikationsprotokoll ermöglicht, bei dem die WAN-Agenten den Status melden, Aktionen durchführen und auf die Anforderungen des GFI LanGuard KI-Servers reagieren. Die GFI LanGuard KI-Server können Befehle an Agenten ausgeben, die bestätigt oder möglicherweise Fehlerantworten basierend auf Erfolg oder Misserfolg auslösen.

FAQs zur WAN-Agent-Scanzeitüberschreitung

Wie funktioniert der Zähler für die WAN-Agent-Offline-Zeitüberschreitung?

Die Einstellung zur WAN-Agent-Scanzeitüberschreitung steuert, wie lange entfernte Netzwerkscans laufen können, bevor sie ablaufen. Diese Einstellung wird zentral auf dem GFI LanGuard KI-Server verwaltet und stellt sicher, dass WAN-Agent-Scans nicht unbegrenzt laufen, indem eine maximale Dauergrenze durchgesetzt wird.

Setzt die Abwesenheit der Verbindung nach der Zeitüberschreitung fort?

Sobald die Zeitüberschreitung abgelaufen ist, beendet der GFI LanGuard KI-Server die Verfolgung des Scanjobs. Der WAN-Agent scannt jedoch weiterhin unabhängig. Wenn der Scan abgeschlossen ist, sendet der WAN-Agent die Ergebnisse an den Server zurück, der sie verarbeitet und aktualisiert, obwohl der Job abgebrochen wurde.

Wann und wie wird der Agent nach einer Zeitüberschreitung neu gestartet?

Die Scanzeitüberschreitung betrifft nur das Job-Tracking auf der Serverseite, nicht den WAN-Agenten. Der WAN-Agent läuft weiterhin normal und wird aufgrund dieser Zeitüberschreitung nicht neu gestartet.

Wer zählt die Zeit? Der Agent, Relay oder Server?

Der GFI LanGuard KI-Server verfolgt und erzwingt die Zeitüberschreitung und führt den Timer für die Dauer, die jeder WAN-Agent-Scan läuft.

Wer entscheidet, wann die Zeit abgelaufen ist? Der Server, Agent oder Relay?

Der GFI LanGuard KI-Server entscheidet und steuert die Zeitüberschreitungsdauer für jeden WAN-Agent-Scanjob.