FirePOWER-Benutzeridentität: Migration vom Benutzer-Agent zur Identity Services Engine

Einführung

In zukünftigen Versionen ist der FirePOWER User Agent nicht mehr verfügbar. Sie wird durch Identity Services Engine (ISE) oder Identity Services Engine (ISE-PIC) ersetzt. Wenn Sie derzeit Benutzer-Agent verwenden und eine Migration auf die ISE in Betracht ziehen, enthält dieses Dokument Überlegungen und Strategien für Ihre Migration.

Übersicht über die Benutzeridentität

Derzeit gibt es zwei Methoden, um Benutzeridentitätsinformationen aus der vorhandenen Identitätsinfrastruktur zu extrahieren: Integration von User Agent und ISE.

Benutzer-Agent

User Agent ist eine Anwendung, die auf einer Windows-Plattform installiert ist. Für den Zugriff auf Benutzeranmeldeereignisse (Ereignistyp 4624) ist das WMI-Protokoll (Windows Management Instrumentation) erforderlich, und die Daten werden dann in einer lokalen Datenbank gespeichert. Benutzer-Agent kann die Anmeldeereignisse auf zwei Arten abrufen: aktualisiert, wenn sich der Benutzer in Echtzeit anmeldet (nur Windows Server 2008 und 2012), oder die Daten für jedes konfigurierbare Intervall abgefragt werden. Ebenso sendet der User Agent aus Active Directory (AD) empfangene Daten in Echtzeit an das FirePOWER Management Center (FMC) und sendet regelmäßig Stapel von Anmeldedaten an FMC.

Anmeldungstypen, die von User Agent erkannt werden können, umfassen die direkte Anmeldung bei einem Host oder über Remote Desktop. Anmeldung zur Dateifreigabe; Anmeldung des Computerkontos. Andere Anmeldetypen wie Citrix, Netzwerkanmeldungen und Kerberos-Anmeldungen werden vom User Agent nicht unterstützt.

Der Benutzer-Agent verfügt über eine optionale Funktion, um festzustellen, ob sich der zugeordnete Benutzer abgemeldet hat. Wenn die Abmeldeprüfung aktiviert ist, wird regelmäßig überprüft, ob der Prozess "explorer.exe" auf jedem zugeordneten Endpunkt ausgeführt wird. Wenn der ausgeführte Prozess nach 72 Stunden nicht erkannt werden kann, wird die Zuordnung für diesen Benutzer entfernt.

Identity Services Engine

Identity Services Engine (ISE) ist ein robuster AAA-Server, der die Netzwerkanmeldesitzungen des Benutzers verwaltet. Da die ISE direkt mit Netzwerkgeräten wie Switches und Wireless-Controllern kommuniziert, hat sie Zugriff auf aktuelle Daten zu Benutzeraktivitäten und ist somit eine bessere Identitätsquelle als der Benutzer-Agent. Wenn sich ein Benutzer bei einem Endpunkt anmeldet, stellt er normalerweise automatisch eine Verbindung zum Netzwerk her. Wenn die 802.1x-Authentifizierung für das Netzwerk aktiviert ist, erstellt die ISE eine Authentifizierungssitzung für diesen Benutzer und hält sie aufrecht, bis sich der Benutzer vom Netzwerk abmeldet. Wenn die ISE in das FMC integriert ist, leitet sie die Benutzer-IP-Zuordnung

(zusammen mit anderen von der ISE erfassten Daten) an das FMC weiter.

ISE kann über pxGrid in FMC integriert werden. pxGrid ist ein Protokoll zur Zentralisierung der Verteilung von Sitzungsinformationen zwischen ISE-Servern und mit anderen Produkten. Bei dieser Integration fungiert die ISE als pxGrid-Controller, und das FMC abonniert den Controller, um Sitzungsdaten zu empfangen (das FMC veröffentlicht außer bei der später beschriebenen Problembehebung keine Daten an die ISE). Die Daten werden an Sensoren weitergeleitet, um die Benutzererkennung zu erreichen.

Identity Services Engine Passive Identity Connector (ISE-PIC) ist im Wesentlichen eine ISE-Instanz mit eingeschränkter Lizenz. ISE-PIC führt keine Authentifizierung durch, sondern fungiert stattdessen als zentraler Hub für verschiedene Identitätsquellen im Netzwerk, sammelt die Identitätsdaten und stellt sie den Teilnehmern zur Verfügung. ISE-PIC ähnelt Benutzer Agent insofern, als es WMI auch verwendet, um Anmeldereignisse von AD zu sammeln, jedoch mit robusteren Funktionen, die als Passive Identity bezeichnet werden. Sie ist auch über pxGrid in FMC integriert.

Überlegungen zur Migration

Lizenzierungsanforderungen

Für das FMC sind keine zusätzlichen Lizenzen erforderlich. Identity Services Engine erfordert eine Lizenz, wenn sie nicht bereits in der Infrastruktur bereitgestellt wird. Weitere Einzelheiten finden Sie im Dokument zum Cisco ISE-Lizenzierungsmodell. Der ISE Passive ID Connector ist ein bereits in der vollständigen ISE-Bereitstellung vorhandener Funktionssatz, daher sind bei einer vorhandenen ISE-Bereitstellung keine zusätzlichen Lizenzen erforderlich. Weitere Informationen zur neuen oder separaten Bereitstellung von ISE-PIC finden Sie im Cisco ISE-PIC-Lizenzierungsdokument.

SSL-Zertifikat

Während User Agent für die Kommunikation mit FMC und Active Directory keine Public Key Infrastructure (PKI) benötigt, erfordert die ISE- oder ISE-PIC-Integration SSL-Zertifikate, die von ISE und FMC nur zu Authentifizierungszwecken gemeinsam genutzt werden. Die Integration unterstützt Zertifikate, die von der Zertifizierungsstelle signiert und selbstsigniert sind, vorausgesetzt, dass den Zertifikaten sowohl "Server Authentication" als auch "Client Authentication" EKU (Extention Key Usage) hinzugefügt werden.

Identitätsquellenabdeckung

Der Benutzer-Agent deckt nur Windows-Anmeldeereignisse von Windows-Desktops mit abfragebasierter Abmeldeerkennung ab. ISE-PIC umfasst die Windows Desktop-Anmeldung sowie zusätzliche Identitätsquellen wie AD Agent, Kerberos SPAN, Syslog Parser und Terminal Services Agent (TSA). Die vollständige ISE ist vollständig von der ISE-PIC-Funktion abgedeckt, einschließlich Netzwerkauthentifizierung von Nicht-Windows-Workstations und Mobilgeräten sowie weiteren Funktionen.

	Benutzer-Agent	ISE-PIC	ISE
Active Directory-Desktop-Anmeldung	Ja	Ja	Ja
Netzwerkanmeldung	Nein	Nein	Ja

Endgeräteerkennung	Ja	Ja	Ja
InfoBlox/IPAMs	Nein	Ja	Ja
LDAP	Nein	Ja	Ja
Sichere Web-Gateways	Nein	Ja	Ja
REST-API-Quellen	Nein	Ja	Ja
Syslog-Parser	Nein	Ja	Ja
Netzwerkbereich	Nein	Ja	Ja

End-of-Life von Benutzer-Agent

Die letzte Version von FirePOWER zur Unterstützung von User Agent ist 6.6. Diese Warnung gibt an, dass User Agent deaktiviert werden muss, bevor ein Upgrade auf spätere Versionen durchgeführt werden kann. Wenn ein Upgrade auf eine Version über 6.6 erforderlich ist, muss die Migration vom Benutzer-Agent auf die ISE oder ISE-PIC vor dem Upgrade abgeschlossen sein. Weitere Informationen finden Sie im Konfigurationshandbuch für Benutzeragenten.

Kompatibilität

Lesen Sie bitte den Kompatibilitätsleitfaden für Firepower-Produkte, um sicherzustellen, dass die Softwareversionen, die an der Integration beteiligt sind, kompatibel sind. Beachten Sie, dass bei zukünftigen Firepower-Versionen die Unterstützung für spätere ISE-Versionen möglicherweise spezielle Patch-Level erfordert.

Migrationsstrategie

Die Migration von User Agent zu ISE oder ISE-PIC erfordert sorgfältige Planung, Durchführung und Tests, um einen reibungslosen Übergang der Benutzeridentitätsquelle für FMC zu gewährleisten und jegliche Beeinträchtigung des Benutzerdatenverkehrs zu vermeiden. Dieser Abschnitt enthält Best Practices und Empfehlungen für diese Aktivität.

Vorbereitung auf die Migration

Die nächsten Schritte können vor dem Wechsel von User Agent zur ISE-Integration durchgeführt werden.

Schritt 1: Konfigurieren Sie ISE oder ISE-PIC, um PassiveID zu aktivieren, und richten Sie die WMI-Verbindung mit Active Directory ein. Weitere Informationen finden Sie im ISE-PIC Administration Guide.

Schritt 2: Erstellen Sie das Identitätszertifikat des FMC. Dabei kann es sich entweder um ein vom FMC ausgestelltes selbstsigniertes Zertifikat oder um ein vom FMC erstelltes Zertifikat (Certificate Signing Request, CSR) handeln, das von einer privaten oder öffentlichen Zertifizierungsstelle (Certificate Authority, CA) unterzeichnet wird. Das selbstsignierte Zertifikat oder das Stammzertifikat der CA muss auf der ISE installiert sein. Weitere Informationen finden Sie im ISE- und FMC-Integrationsleitfaden.

Schritt 3: Installieren Sie das CA-Root-Zertifikat, das das pxGrid-Zertifikat der ISE signiert hat (bzw. das pxGrid-Zertifikat, falls es selbst signiert ist) auf dem FMC. Weitere Informationen finden Sie im ISE- und FMC-Integrationsleitfaden.

Anpassungsprozess

Die FMC-ISE-Integration kann nicht konfiguriert werden, ohne die User Agent-Konfiguration auf FMC zu deaktivieren, da sich die beiden Konfigurationen gegenseitig ausschließen. Dies kann sich möglicherweise auf die Benutzer während der Änderung auswirken. Es wird empfohlen, diese Schritte während des Wartungsfensters auszuführen.

Schritt 1: Aktivieren und überprüfen Sie die FMC-ISE-Integration. Weitere Informationen finden Sie im ISE- und FMC-Integrationsleitfaden.

Schritt 2: Stellen Sie sicher, dass Benutzeraktivitäten dem FMC gemeldet werden, indem Sie auf der FMC-Seite **Analysis > User > User Activities** (Analyse > Benutzer > Benutzeraktivitäten) navigieren.

Schritt 3: Überprüfen Sie, ob die Benutzer-IP-Zuordnung und die Benutzergruppenzuordnung auf verwalteten Geräten auf
Analyse > Verbindungen > Ereignisse > Tabellenansicht von Verbindungsereignissen.

Schritt 4: Ändern Sie die Zugriffskontrollrichtlinie, um die Aktion zur **Überwachung** vorübergehend auf Regeln zu ändern, die Datenverkehr je nach Benutzername oder Benutzergruppenbedingung blockieren. Bei Regeln, die Datenverkehr basierend auf dem Initiator-Benutzer oder der Gruppe zulassen, erstellen Sie eine doppelte Regel, die den Datenverkehr ohne Benutzerkriterien zulässt, und deaktivieren Sie dann die ursprüngliche Regel. Dieser Schritt soll sicherstellen, dass geschäftskritischer Datenverkehr während der Testphase nach dem Wartungsfenster nicht beeinträchtigt wird.

Schritt 5: Beachten Sie nach dem Wartungsfenster während der normalen Geschäftszeiten die Connection Events auf FMC, um die Benutzer-IP-Zuordnung zu überwachen. Beachten Sie, dass Verbindungsereignisse Benutzerinformationen nur anzeigen, wenn eine aktivierte Regel Benutzerdaten erfordert. Daher wird die Monitoraktion im letzten Schritt empfohlen.

Schritt 6: Wenn der gewünschte Status erreicht ist, kehren Sie einfach die an den Zugriffskontrollrichtlinien vorgenommenen Änderungen um und schieben Sie die Richtlinienbereitstellung auf die verwalteten Geräte.

Zusätzliche Informationen

- Video-Tutorial: Benutzer-Agent-Übergang zu ISE-PIC
- Administratoranleitung für die Cisco ISE 2.4: Lizenzierung
- Installations- und Administratoranleitung für ISE-PIC (Identity Services Engine Passive Identity Connector), Version 2.2
- Konfigurationsanleitung für Benutzer-Agent
- Cisco FirePOWER-Kompatibilitätsleitfaden
- Konfigurieren der ISE 2.4- und FMC 6.2.3 pxGrid-Integration