Probleme mit der Transparenz der sicheren Client-Identität beim MX75-Netzwerktunnel bei sicherem Zugriff

Inhalt

Problem

Wenn Endpunkte mit sicherem Client hinter einem MX75-Netzwerktunnel bereitgestellt werden, der eine Verbindung mit sicherem Zugriff herstellt, sind die Roaming-Client- und Benutzeridentitäten im System nicht richtig sichtbar. Die folgenden spezifischen Verhaltensweisen werden beobachtet:

- Backoff-Einstellungen, die zur Priorisierung von Secure Client über Netzwerk-Tunnelverbindungen konfiguriert wurden, funktionieren nicht wie erwartet, wenn sich die Endpunkte hinter dem MX75 befinden.
- Domänenbasierte Verkehrssteuerungsregeln gelten nicht, da der Datenverkehr nur der Netzwerktunnelidentität und nicht dem Roaming-Client zugewiesen wird.
- Bei der Aktivitätssuche werden unvollständige Informationen zum Quellstandort angezeigt. Dabei wird nur die Netzwerktunnelidentität angezeigt, während Benutzer- und Roaming-Client-Identitäten ausgelassen werden.
- Identitätsbasierte Verkehrssteuerungsregeln (z. B. auf Basis von Active Directory-Benutzern oder Roaming-Client-Identität) gelten nicht für den Datenverkehr, der den MX75-Tunnel durchquert

Dieses Verhalten verhindert eine ordnungsgemäße Identitätstrennung und Richtlinienanwendung für Endpunkte, die über die Netzwerk-Tunnelinfrastruktur verbunden sind.

Umwelt

- Cisco Secure Access-Bereitstellung
- MX75-Appliance mit Netzwerk-Tunnel-Konfiguration für sicheren Zugriff
- Auf allen Endgeräten installierte Secure Client-Agenten

- Backoff-Einstellungen auf Roaming-Clients deaktiviert, um Secure Client über Netzwerk-Tunnelverbindungen zu priorisieren
- Verkehrslenkungsregeln für domänenbasiertes Routing
- Identitätsbasierte Richtlinien, konfiguriert für Active Directory-Benutzer und Roaming-Clients

Auflösung

Das Problem wurde durch die Implementierung einer Workaround-Konfiguration mithilfe eines registrierten Netzwerks behoben, anstatt sich auf die Roaming-Identitätstransparenz durch den MX75-Netzwerktunnel zu verlassen.

Workaround-Implementierung

Schritt 1: RSM (Roaming Security Module) mit registriertem Netzwerk konfigurieren

Ersetzen Sie die vorhandene Netzwerk-Tunnel-Konfiguration durch eine RSM-Bereitstellung in Kombination mit einer Konfiguration für ein registriertes Netzwerk. Diese Konfiguration ermöglicht die korrekte Identitätszuweisung und Richtlinienanwendung.

Phase 2: Identitätstransparenz überprüfen

Überprüfen Sie nach der Implementierung der Konfiguration des registrierten Netzwerks Folgendes:

- Die Benutzeridentitäten werden in der Aktivitätssuche richtig angezeigt.
- Roaming-Client-Identitäten sind sichtbar und korrekt zugeordnet
- Verkehrslenkungsregeln basierend auf Benutzer- und Client-Identitätsfunktion wie erwartet

Schritt 3: Funktionen zur Prüfung der Verkehrssteuerung

Überprüfen Sie, ob domänenbasierte Verkehrssteuerungsregeln und identitätsbasierte Richtlinien in der neuen Konfiguration korrekt angewendet werden.

Alternativer Ansatz

Bei Umgebungen, in denen eine Identitätstrennung über private Netzwerke nicht erforderlich ist, sollten Sie die Implementierung von RSM (Internet Configuration) in Betracht ziehen. Bei diesem Ansatz wird RSM-Datenverkehr direkt an das Internet gesendet, anstatt ihn über den privaten Netzwerktunnel zu leiten. So wird eine angemessene Identitätstransparenz sichergestellt und die Sicherheitskontrollen aufrechterhalten.

Technische Analyse

Während der Fehlerbehebung wurden Diagnosedaten unter Verwendung von policy.test.sse.cisco.com gesammelt, um das Identitätszuweisungsverhalten zu demonstrieren, wenn sich die Endpunkte hinter dem MX75-Tunnel befanden. Die Analyse hat bestätigt, dass das Routing von Roaming-Identitäten durch einen Netzwerktunnel zwar technisch möglich ist, für dieses spezielle Bereitstellungsszenario jedoch nicht empfohlen oder unterstützt wird.

Ursache

Die Ursache hängt damit zusammen, wie Secure Access die Identitätszuweisung handhabt, wenn der Datenverkehr durch die Netzwerk-Tunnelinfrastruktur fließt. Wenn Endpunkte eine Verbindung über den MX75-Netzwerktunnel herstellen, ordnet das System den gesamten Datenverkehr der Tunnelidentität zu, anstatt die einzelnen Roaming-Client- und Benutzeridentitäten beizubehalten. Dieses Verhalten ist für Netzwerk-Tunnelverbindungen konzipiert, steht jedoch im Widerspruch zu der Anforderung nach individueller Identitätstransparenz und Richtlinienanwendung.

Obwohl es technisch machbar ist, Roaming-Identitäten durch Netzwerktunnel zu routen, wird diese Konfiguration aufgrund der oben beschriebenen Einschränkungen bei der Identitätszuweisung nicht empfohlen oder als Standard-Betriebsablauf unterstützt.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.