Warnungsregelaktion konfigurieren

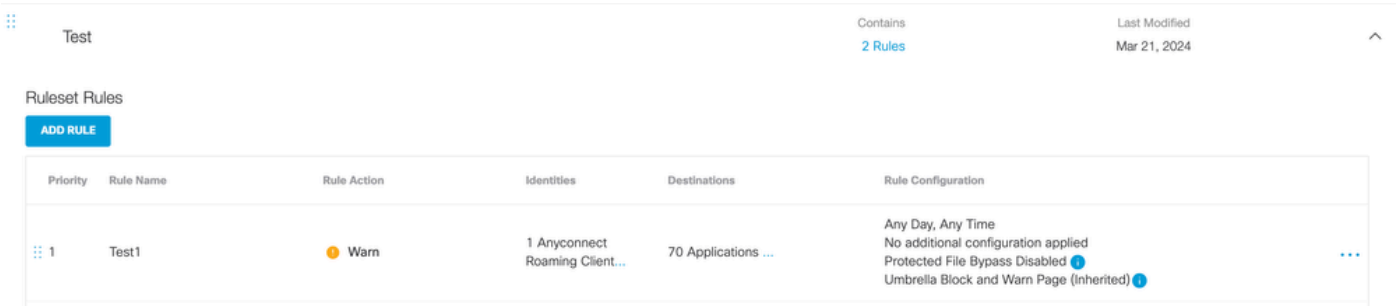
Inhalt

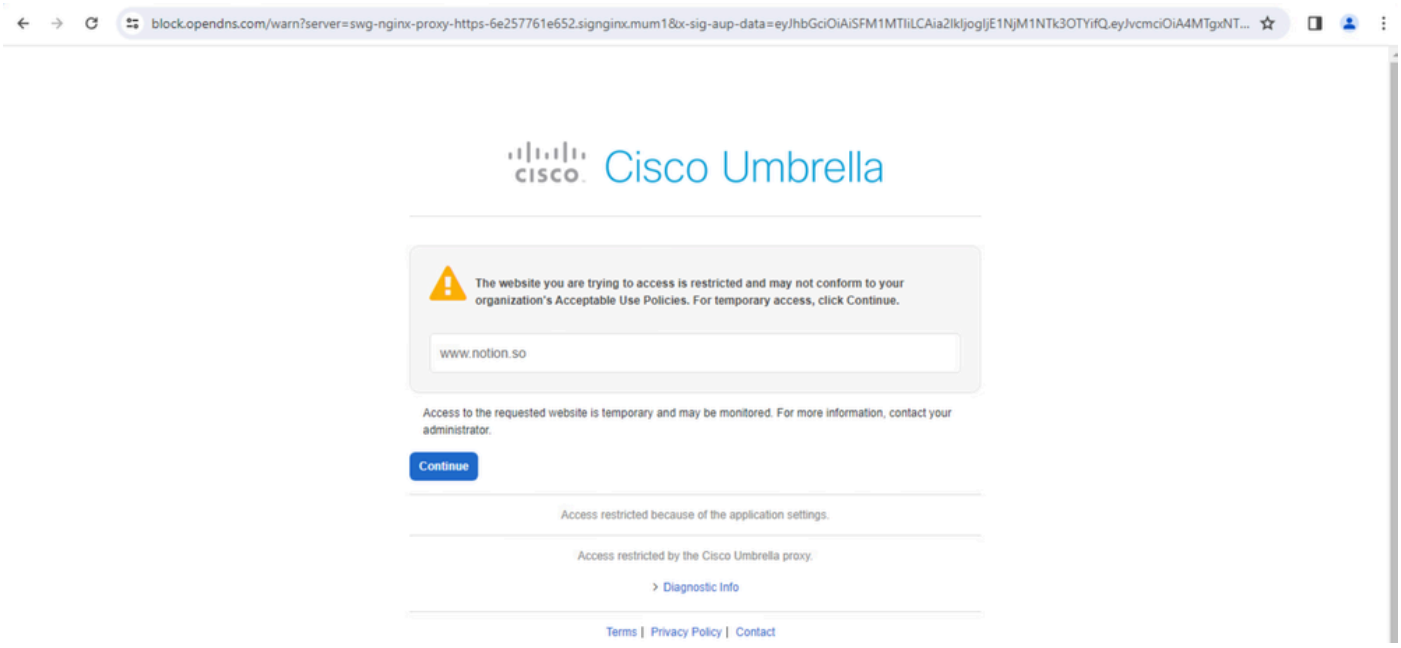
Einleitung

Dieses Dokument beschreibt ein umfassendes Verständnis der Warnungsregel-Aktionsfunktion, ihrer Konfiguration und der zugehörigen Einschränkungen in Cisco Umbrella.

Überblick

Wenn ein Benutzer versucht, auf eine Website zuzugreifen, die in der Kategorie "Warn" unter "Cisco Umbrella" aufgeführt ist, wird eine Warn-Seite angezeigt. Um fortzufahren, müssen Benutzer durch die Warn-Seite klicken.



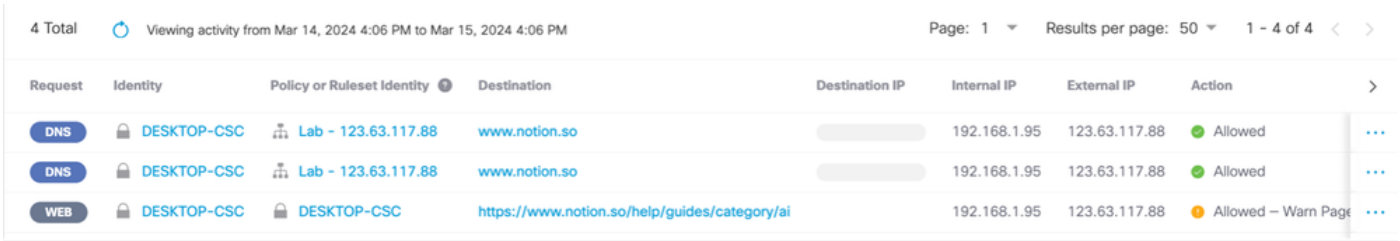


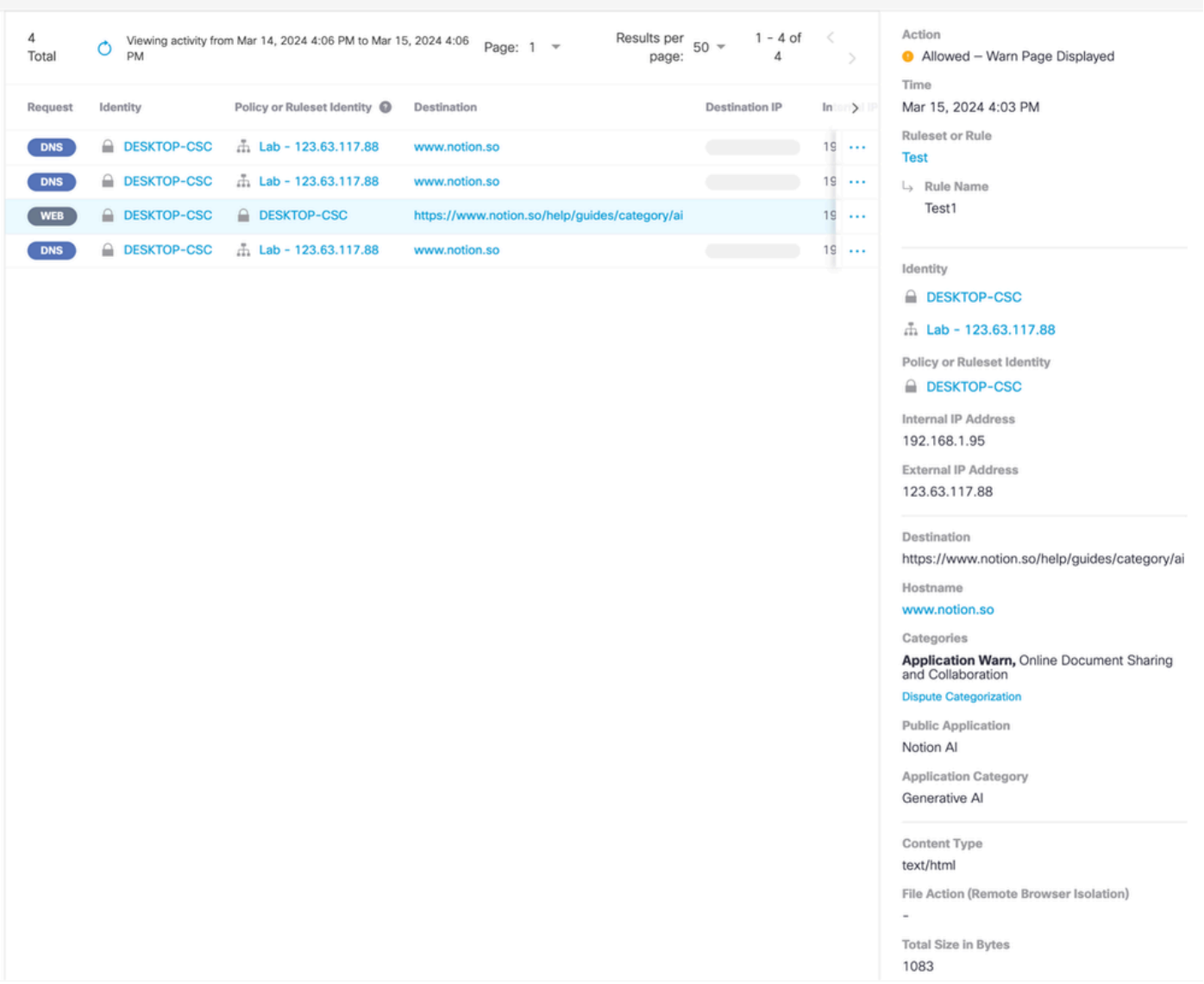
Zugriffsdauer

Wenn Sie durch die Warn-Seite klicken, erhalten Sie für eine begrenzte Dauer von einer Stunde Zugriff auf das gewünschte Ziel. Nach Ablauf dieses Zeitraums wird die Warnungsseite erneut angezeigt, sodass die Benutzer erneut auf die Seite klicken müssen, um den Zugriff fortzusetzen.

Aktivitätsbericht - Übersicht

Interaktionen mit Warnungsseiten werden in Umbrellas Aktivitätsberichten protokolliert, sodass Administratoren Einblicke in Benutzerinteraktionen und Warnungen erhalten, die durch die Warnungsregelaktion ausgelöst werden.





Einschränkungen der Zielliste

Durch Aktivieren der Funktion Warnungsseite wird der Zugriff auf Ziellisten eingeschränkt. Benutzer können die Option "Zielliste" für Websites, die unter "Warnung" kategorisiert sind, nicht auswählen.

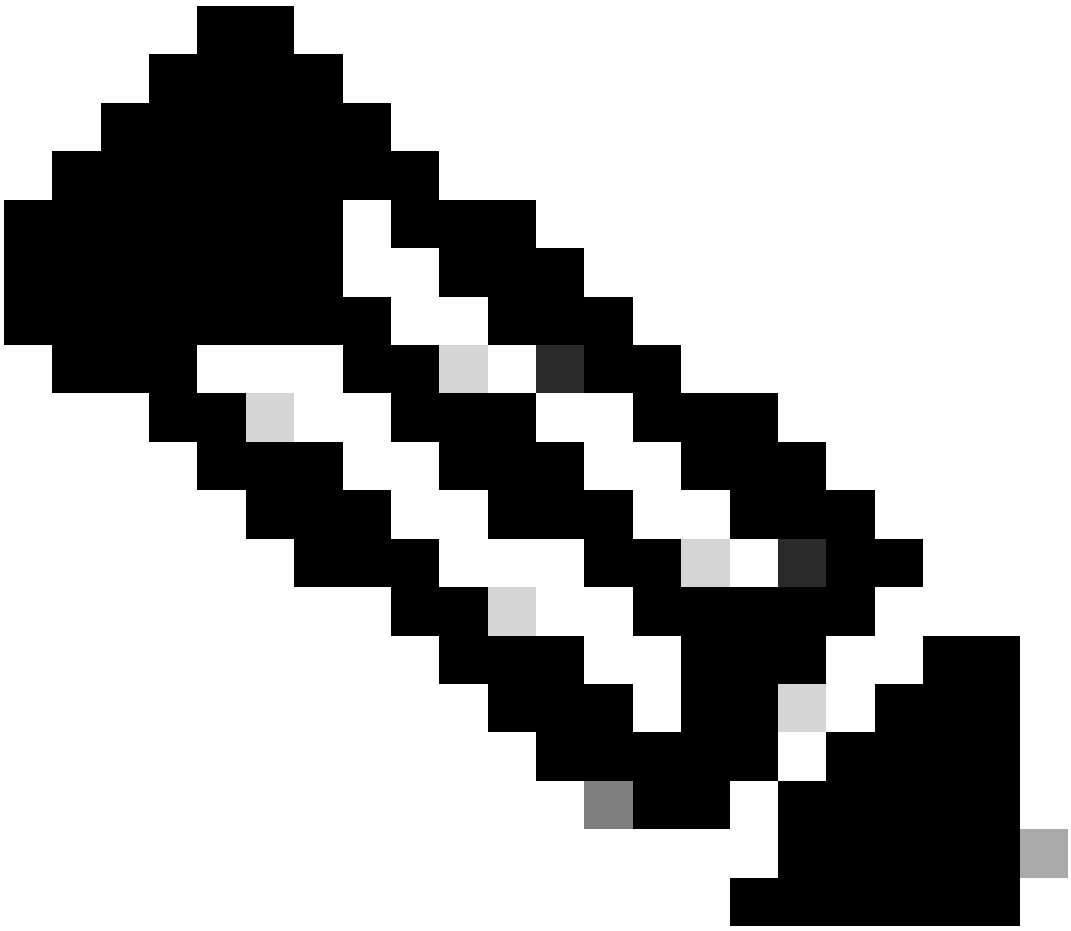
Aktivieren von HTTPS-Überprüfung

Um die Warnungsseitenfunktion wirksam durchzusetzen, muss HTTPS-Inspektion in Cisco Umbrella aktiviert sein. HTTPS Inspection entschlüsselt und überprüft HTTPS-Datenverkehr und aktiviert Umbrella, um Warnungsseiten für verschlüsselte Verbindungen durchzusetzen.

Erstellen einer benutzerdefinierten Warnungsseite

Administratoren können eine benutzerdefinierte Warnseite mit personalisiertem Messaging erstellen. Diese benutzerdefinierte Warnungsseite kann beim Hinzufügen von Regeln zu einem Regelsatz ausgewählt werden, um Benutzern eine maßgeschneiderte Warnungserfahrung zu bieten.

Detaillierte Anweisungen zum Erstellen einer benutzerdefinierten Warnungsseite und weitere Informationen zur Konfiguration der Warnungsregel finden Sie in der offiziellen Dokumentation: Benutzerdefinierte Warnungsseite erstellen.



> Anmerkung: Alle Ausnahmen von der Liste der selektiven Entschlüsselung beeinflussen die Fähigkeit des Proxys, bestimmte Richtlinien und Funktionen durchzusetzen. Die Warnungsseite ist eine davon.

Schlussfolgerung

Um effektive Sicherheitsrichtlinien in Cisco Umbrella zu implementieren, müssen Sie die Konfiguration der Warnungsregel und die zugehörigen Einschränkungen kennen. Mithilfe von

Warn-Seiten und HTTPS-Inspektion können Organisationen ihren Sicherheitsstatus verbessern und sicherstellen, dass Benutzer sicher im Internet surfen.

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.