Wie konfiguriere ich IP-Spoofing?

Inhalt

Frage

Wie konfiguriere ich IP-Spoofing?

Umgebung: Cisco Web Security Appliance (WSA), alle Versionen von AsyncOS

Zusammenfassung:

Bei einer herkömmlichen Proxy-Bereitstellung wird die IP-Adresse des Clients durch die des Proxy-/Cache-Servers ersetzt. Dies bietet inhärente Sicherheit, indem die Adresse des Endbenutzers maskiert wird. In einigen Fällen erfordern bestimmte Webanwendungen jedoch Zugriff auf die IP-Adresse des ursprünglichen Clients.

Durch die Implementierung der IP-Spoofing-Funktion in der Cisco Web Security Appliance (WSA) und die Konfiguration der entsprechenden WCCP-Servicegruppen auf einem Cisco IOS-Gerät ist es möglich, die IP-Adresse des Clients anstelle der IP-Adresse der WSA für Webanwendungen anzuzeigen. Im folgenden Dokument werden die erforderlichen Konfigurationsschritte für diese Implementierung beschrieben.

Beschreibung:

Zur Implementierung der Funktion "IP Spoofing" mussten auf einem Cisco IOS® Router zwei eindeutige WCCP-Servicegruppen erstellt werden. Die erste "Web-Cache"-Gruppe des WCCP leitet HTTP/Port 80-Datenverkehr vom Benutzer an die WSA um. Spezifische Zugriffskontrolllisten können konfiguriert werden (wie im Beispiel unten gezeigt), um zu kontrollieren, welche Benutzer durch die Cisco Web Security Appliance geschützt sind. Die Benutzeroberfläche des Routers ist so konfiguriert, dass eingehender Datenverkehr an diese WCCP-Servicegruppe umgeleitet wird.

Die zweite WCCP-Servicegruppe muss als dynamische Service-ID definiert werden (z. B. Service-ID 95). Auch hier wird eine Zugriffsliste verwendet, um zu steuern, welche Benutzer geschützt sind (d. h. das gesamte System umgehen zu lassen). Für den zurückkehrenden Web-Datenverkehr wird die externe Schnittstelle des Routers so konfiguriert, dass der eingehende Datenverkehr an die WCCP-Servicegruppe 95 umgeleitet wird.