Konfigurationsbeispiel zum SSL VPN Client (SVC) unter ASA mit ASDM

Inhalt

Einleitung

Die SSL-VPN-Technologie (Secure Socket Layer Virtual Private Network) ermöglicht die sichere Verbindung mit einem internen Unternehmensnetzwerk von einem beliebigen Standort aus. Dazu stehen folgende Methoden zur Verfügung:

- Clientless SSL VPN (WebVPN) - Stellt einen Remoteclient bereit, der einen SSL-fähigen Webbrowser benötigt, um auf HTTP- oder HTTPS-Webserver in einem lokalen Unternehmensnetzwerk (LAN) zuzugreifen. Darüber hinaus ermöglicht das Clientless-SSL-VPN den Zugriff auf Windows-Dateien, die über das CIFS-Protokoll (Common Internet File System) durchsucht werden. Outlook Web Access (OWA) ist ein Beispiel für den HTTP-Zugriff.

  Weitere Informationen zum SSL VPN ohne Client finden Sie unter Clientless SSL VPN (WebVPN) im ASA-Konfigurationsbeispiel.

- Thin-Client SSL VPN (Port Forwarding) - Stellt einen Remote-Client bereit, der ein kleines Java-basiertes Applet herunterlädt und sicheren Zugriff für TCP-Anwendungen (Transmission Control Protocol) ermöglicht, die statische Portnummern verwenden. Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Secure Shell (SSH) und Telnet sind Beispiele für sicheren Zugriff. Da sich Dateien auf dem lokalen Computer ändern, müssen Benutzer über lokale Administratorberechtigungen verfügen, um diese Methode verwenden zu können. Diese SSL VPN-Methode funktioniert nicht mit Anwendungen, die dynamische Portzuweisungen verwenden, z. B. einige FTP-Anwendungen (File Transfer Protocol).

  Weitere Informationen zum Thin-Client SSL VPN finden Sie unter Thin-Client SSL VPN (WebVPN) auf ASA mit ASDM-Konfigurationsbeispiel.

  Hinweis: UDP wird nicht unterstützt.

- SSL VPN Client (Tunnel Mode) - Lädt einen kleinen Client auf die Remote-Workstation herunter und ermöglicht einen sicheren Zugriff auf Ressourcen in einem internen Unternehmensnetzwerk. Sie können den SSL VPN Client (SVC) dauerhaft auf eine Remote-Workstation herunterladen oder den Client entfernen, sobald die sichere Sitzung beendet ist.

In diesem Dokument wird beschrieben, wie der SVC mithilfe des Adaptive Security Device Manager (ASDM) auf einer Adaptive Security Appliance (ASA) konfiguriert wird. Die Befehlszeilen, die sich aus dieser Konfiguration ergeben, sind im Abschnitt Ergebnisse aufgeführt.

Voraussetzungen

Anforderungen

Bevor Sie diese Konfiguration durchführen, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- SVC startet Support von Cisco Adaptive Security Appliance Software Version 7.1 und höher
- Lokale Administratorberechtigungen auf allen Remote-Workstations
- Java- und ActiveX-Steuerelemente auf der Remote-Workstation
- Port 443 wird entlang des Verbindungspfads nicht blockiert.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Adaptive Security Appliance Software Version 7.2(1)
- Cisco Adaptive Security Device Manager 5.2(1)
- Cisco Adaptive Security Appliance der Serie 5510
- Microsoft Windows XP Professional SP 2

Die Informationen in diesem Dokument wurden in einer Laborumgebung entwickelt. Alle Geräte, die in diesem Dokument gestartet wurden, wurden auf ihre Standardkonfiguration zurückgesetzt. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Befehle verstehen. Alle in dieser Konfiguration verwendeten IP-Adressen wurden aus RFC 1918-Adressen in einer Laborumgebung ausgewählt. Diese IP-Adressen können nicht über das Internet geroutet werden und dienen nur Testzwecken.

Netzwerkdiagramm

In diesem Dokument wird die in diesem Abschnitt beschriebene Netzwerkkonfiguration verwendet.

Ein Remote-Benutzer stellt über einen SSL-fähigen Webbrowser eine Verbindung zur IP-Adresse der ASA her. Nach erfolgreicher Authentifizierung wird der SVC auf den Client-Computer heruntergeladen, und der Benutzer kann eine verschlüsselte sichere Sitzung für den vollständigen Zugriff auf alle zulässigen Ressourcen im Unternehmensnetzwerk verwenden.

Vorkonfigurationsaufgaben

Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Weitere Informationen dazu, wie die ASA vom ASDM konfiguriert werden kann, finden Sie unter Zulassen des HTTPS-Zugriffs für ASDM.

  Um von Ihrer Managementstation aus auf die ASDM-Anwendung zuzugreifen, verwenden Sie einen SSL-fähigen Webbrowser, und geben Sie die IP-Adresse des ASA-Geräts ein. Beispiel: https://inside_ip_address, wobei inside_ip_address die Adresse der ASA ist. Sobald ASDM geladen ist, können Sie mit der Konfiguration des SVC beginnen.

- Laden Sie das SSL VPN Client-Paket (sslclient-win*.pkg) von der Cisco Software Download-Website (nur für registrierte Kunden) auf die lokale Festplatte der Verwaltungsstation herunter, von der aus Sie auf die ASDM-Anwendung zugreifen.

WebVPN und ASDM können nicht auf derselben ASA-Schnittstelle aktiviert werden, es sei denn, Sie ändern die Portnummern. Wenn Sie möchten, dass beide Technologien denselben Port (Port 443) auf demselben Gerät verwenden, können Sie ASDM auf der internen Schnittstelle und

WebVPN auf der externen Schnittstelle aktivieren.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Konfigurieren des SSL VPN-Clients auf einem ASA

Führen Sie die folgenden Schritte aus, um den SSL VPN-Client auf einem ASA-Gerät zu konfigurieren:

1. WebVPN-Zugriff auf der ASA aktivieren
2. Installation und Aktivierung des SSL VPN-Clients auf der ASA
3. SVC-Installation auf Clients aktivieren
4. Rekey-Parameter aktivieren

Schritt 1: WebVPN-Zugriff auf der ASA aktivieren

Führen Sie die folgenden Schritte aus, um den WebVPN-Zugriff auf der ASA zu aktivieren:

1. Klicken Sie in der ASDM-Anwendung auf Configuration (Konfiguration) und dann auf VPN (VPN).
2. Erweitern Sie WebVPN, und wählen Sie WebVPN Access aus.
3. Wählen Sie die Schnittstelle aus, für die Sie WebVPN aktivieren möchten, und klicken Sie auf Aktivieren.

Schritt 2: Installation und Aktivierung des SSL VPN-Clients auf der ASA

Führen Sie die folgenden Schritte aus, um den SSL VPN-Client auf dem ASA-Gerät zu installieren und zu aktivieren:

1. Klicken Sie auf Konfiguration und dann auf VPN.
2. Erweitern Sie im Navigationsbereich die Option WebVPN, und wählen Sie SSL VPN Client.
3. Klicken Sie auf Hinzufügen.

   Das Dialogfeld "SSL VPN-Client-Image hinzufügen" wird angezeigt.
4. Klicken Sie auf die Schaltfläche Hochladen.

   Das Dialogfeld Bild hochladen wird angezeigt.

5. Klicken Sie auf die Schaltfläche Lokale Dateien durchsuchen, um eine Datei auf Ihrem lokalen Computer zu suchen, oder klicken Sie auf die Schaltfläche Flash durchsuchen, um eine Datei im Flash-Dateisystem zu suchen.
6. Suchen Sie die Client-Image-Datei, die hochgeladen werden soll, und klicken Sie auf OK.
7. Klicken Sie auf Datei hochladen, und klicken Sie dann auf Schließen.
8. Wenn das Client-Image in Flash geladen wurde, aktivieren Sie das Kontrollkästchen SSL VPN Client aktivieren, und klicken Sie dann auf Anwenden.

   Hinweis: Wenn Sie eine Fehlermeldung erhalten, stellen Sie sicher, dass der WebVPN-Zugriff aktiviert ist. Erweitern Sie im Navigationsbereich die Option WebVPN, und wählen Sie WebVPN Access (WebVPN-Zugriff). Wählen Sie die Schnittstelle aus, für die Sie den Zugriff konfigurieren möchten, und klicken Sie auf Aktivieren.
9. Klicken Sie auf Speichern und dann auf Ja, um die Änderungen zu übernehmen.

Schritt 3: SVC-Installation auf Clients aktivieren

Führen Sie die folgenden Schritte aus, um die SVC-Installation auf Clients zu aktivieren:

1. Erweitern Sie im Navigationsbereich die Option IP Address Management (IP-Adressenverwaltung), und wählen Sie IP Pools (IP-Pools).
2. Klicken Sie auf Hinzufügen, und geben Sie die Werte in die Felder Name, Start-IP-Adresse, End-IP-Adresse und Subnetzmaske ein. Die IP-Adressen, die Sie für die Felder "Start-IP-Adresse" und "End-IP-Adresse" eingeben, müssen aus Subnetzen in Ihrem internen Netzwerk stammen.
3. Klicken Sie auf OK und dann auf Übernehmen.
4. Klicken Sie auf Speichern und dann auf Ja, um die Änderungen zu übernehmen.
5. Erweitern Sie im Navigationsbereich die Option IP Address Management (IP-Adressenverwaltung), und wählen Sie Assignment (Zuweisung).
6. Aktivieren Sie das Kontrollkästchen Interne Adresspools verwenden, und deaktivieren Sie dann die Kontrollkästchen Authentifizierungsserver verwenden und DHCP verwenden.
7. Klicken Sie auf Apply (Anwenden).
8. Klicken Sie auf Speichern und dann auf Ja, um die Änderungen zu übernehmen.
9. Erweitern Sie im Navigationsbereich die Option General (Allgemein), und wählen Sie Tunnel Group (Tunnelgruppe).
10. Wählen Sie die Tunnelgruppe aus, die Sie verwalten möchten, und klicken Sie auf Bearbeiten.

11. Klicken Sie auf die Registerkarte Client Address Assignment (Client-Adressenzuweisung), und wählen Sie den neu erstellten IP-Adresspool aus der Liste Available Pools (Verfügbare Pools) aus.

12. Klicken Sie auf Hinzufügen und dann auf OK.

13. Klicken Sie im ASDM-Anwendungsfenster auf Apply.

14. Klicken Sie auf Speichern und dann auf Ja, um die Änderungen zu übernehmen.

Schritt 4: Rekey-Parameter aktivieren

So aktivieren Sie rekey-Parameter:

1. Erweitern Sie im Navigationsbereich die Option General (Allgemein), und wählen Sie Group Policy (Gruppenrichtlinie).

2. Wählen Sie die Richtlinie aus, die Sie auf diese Gruppe von Clients anwenden möchten, und klicken Sie auf Bearbeiten.

3. Deaktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen Tunneling-Protokolle übernehmen, und aktivieren Sie das Kontrollkästchen WebVPN.

4. Klicken Sie auf die Registerkarte WebVPN, klicken Sie auf die Registerkarte SSL VPN Client, und wählen Sie die folgenden Optionen aus:

    a. Deaktivieren Sie für die Option SSL VPN Client verwenden das Kontrollkästchen Vererben, und klicken Sie auf das Optionsfeld Optional.

    Mit dieser Option kann der Remote-Client auswählen, ob der SVC heruntergeladen werden soll oder nicht. Mit der Option Immer wird sichergestellt, dass der SVC bei jeder SSL VPN-Verbindung auf die Remote-Workstation heruntergeladen wird.

    b. Deaktivieren Sie für die Option Installationsprogramm auf Client-System beibehalten das Kontrollkästchen Erben, und klicken Sie auf das Optionsfeld Ja.

    Durch diese Aktion kann die SVC-Software auf dem Client-Computer verbleiben. Daher muss die ASA die SVC-Software nicht jedes Mal auf den Client herunterladen, wenn eine Verbindung hergestellt wird. Diese Option ist eine gute Wahl für Remote-Benutzer, die häufig auf das Unternehmensnetzwerk zugreifen.

    c. Deaktivieren Sie für die Option "Neuverhandlungsintervall" das Kontrollkästchen Erben, deaktivieren Sie das Kontrollkästchen Unbegrenzt, und geben Sie die Anzahl der Minuten bis zur erneuten Eingabe ein.

    Die Sicherheit wird verbessert, indem die Gültigkeitsdauer eines Schlüssels begrenzt wird.

    d. Deaktivieren Sie für die Option Neuverhandlungsmethode das Kontrollkästchen Vererben, und klicken Sie auf das Optionsfeld SSL. Bei einer Neuverhandlung kann

der vorhandene SSL-Tunnel oder ein neuer Tunnel, der ausdrücklich für eine Neuverhandlung erstellt wurde, verwendet werden.

Die Attribute für den SSL VPN-Client sollten wie in diesem Bild dargestellt konfiguriert werden:

5. Klicken Sie auf OK und dann auf Übernehmen.
6. Klicken Sie auf Speichern und dann auf Ja, um die Änderungen zu übernehmen.

Ergebnisse

Der ASDM erstellt die folgenden Befehlszeilenkonfigurationen:

Ciscoasa

<#root>

```
ciscoasa(config)#
```

show run

```
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
```

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
!

!--- Group Policy Statements

group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn

!--- Enable the SVC for WebVPN

 webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
username cisco password 53QNetqK.Kqqfshe encrypted privilege 15
!
http server enable
http 10.2.2.0 255.255.255.0 inside
!
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- Tunnel Group and Group Policy using the defaults here

tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool CorporateNet
 default-group-policy GroupPolicy1
!
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
!
telnet timeout 5
ssh 172.22.1.0 255.255.255.0 outside
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
```

```
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global

!--- Enable webvpn and the select the SVC client

webvpn
 enable outside
 svc image disk0:/sslclient-win-1.1.1.164.pkg 1
 svc enable

!--- Provide list for access to resources

 url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
 url-list ServerList "BrowseServer" cifs://10.2.2.2 2
 tunnel-group-list enable

prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f
: end
```

Anpassen der Konfiguration

Die unter Konfigurieren des SSL VPN-Clients auf einem ASA beschriebenen Verfahren verwenden die ASA-Standardnamen für Gruppenrichtlinien (GroupPolicy1) und Tunnelgruppen (DefaultWebVPNGroup) wie in diesem Bild dargestellt:

In diesem Verfahren wird beschrieben, wie Sie eigene benutzerdefinierte Gruppenrichtlinien und Tunnelgruppen erstellen und diese gemäß den Sicherheitsrichtlinien Ihrer Organisation miteinander verknüpfen.

Führen Sie zum Anpassen der Konfiguration die folgenden Schritte aus:

1. Erstellen einer benutzerdefinierten Gruppenrichtlinie
2. Erstellen einer benutzerdefinierten Tunnelgruppe
3. Erstellen Sie einen Benutzer, und fügen Sie diesen Benutzer zu Ihrer benutzerdefinierten Gruppenrichtlinie hinzu.

Schritt 1: Erstellen einer benutzerdefinierten Gruppenrichtlinie

Gehen Sie wie folgt vor, um eine benutzerdefinierte Gruppenrichtlinie zu erstellen:

1. Klicken Sie auf Konfiguration und dann auf VPN.
2. Erweitern Sie Allgemein, und wählen Sie Gruppenrichtlinie aus.

3. Klicken Sie auf Hinzufügen, und wählen Sie Interne Gruppenrichtlinie aus.
4. Geben Sie im Feld Name einen Namen für die Gruppenrichtlinie ein.

   In diesem Beispiel wurde der Name der Gruppenrichtlinie in SalesGroupPolicy geändert.
5. Deaktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen Tunneling-Protokolle übernehmen, und aktivieren Sie das Kontrollkästchen WebVPN.
6. Klicken Sie auf die Registerkarte WebVPN, und klicken Sie dann auf die Registerkarte SSL VPN Client.

   In diesem Dialogfeld können Sie auch das Verhalten des SSL VPN-Clients festlegen.
7. Klicken Sie auf OK und dann auf Übernehmen.
8. Klicken Sie auf Speichern und dann auf Ja, um die Änderungen zu übernehmen.

Schritt 2: Erstellen einer benutzerdefinierten Tunnelgruppe

Gehen Sie wie folgt vor, um eine benutzerdefinierte Tunnelgruppe zu erstellen:

1. Klicken Sie auf die Schaltfläche Konfiguration und dann auf VPN.
2. Erweitern Sie General (Allgemein), und wählen Sie Tunnel Group (Tunnelgruppe).
3. Klicken Sie auf Hinzufügen, und wählen Sie WebVPN Access aus.
4. Geben Sie im Feld Name einen Namen für Ihre Tunnelgruppe ein.

   In diesem Beispiel wurde der Tunnelgruppenname in SalesForceGroup geändert.
5. Klicken Sie auf den Pfeil des Dropdown-Menüs Gruppenrichtlinie, und wählen Sie die neu erstellte Gruppenrichtlinie aus.

   Ihre Gruppenrichtlinie und die Tunnelgruppe sind jetzt verknüpft.
6. Klicken Sie auf die Registerkarte Client Address Assignment (Client-Adressenzuweisung), und geben Sie DHCP-Serverinformationen ein, oder wählen Sie einen lokal erstellten IP-Pool aus.
7. Klicken Sie auf OK und dann auf Übernehmen.
8. Klicken Sie auf Speichern und dann auf Ja, um die Änderungen zu übernehmen.

Schritt 3: Erstellen Sie einen Benutzer, und fügen Sie diesen Benutzer zu Ihrer benutzerdefinierten Gruppenrichtlinie hinzu.

Führen Sie die folgenden Schritte aus, um einen Benutzer zu erstellen und ihn Ihrer benutzerdefinierten Gruppenrichtlinie hinzuzufügen:

1. Klicken Sie auf Konfiguration und dann auf VPN.
2. Erweitern Sie Allgemein, und wählen Sie Benutzer aus.
3. Klicken Sie auf Hinzufügen, und geben Sie Benutzername und Kennwort ein.
4. Klicken Sie auf die Registerkarte VPN Policy (VPN-Richtlinie). Stellen Sie sicher, dass Ihre neu erstellte Gruppenrichtlinie im Feld Gruppenrichtlinie angezeigt wird.

   Dieser Benutzer übernimmt alle Merkmale der neuen Gruppenrichtlinie.
5. Klicken Sie auf OK und dann auf Übernehmen.
6. Klicken Sie auf Speichern und dann auf Ja, um die Änderungen zu übernehmen.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Authentifizierung

Die Authentifizierung für SSL VPN-Clients erfolgt mithilfe einer der folgenden Methoden:

- Cisco Secure ACS Server (Radius)
- NT-Domäne
- Active Directory
- Einmalige Kennwörter
- Digitale Zertifikate
- Smartcards
- Lokale AAA-Authentifizierung

In dieser Dokumentation wird ein lokales Konto verwendet, das auf dem ASA-Gerät erstellt wurde.

Hinweis: Wenn eine Adaptive Security Appliance über mehrere Trustpoints verfügt, die sich die gleiche CA teilen, kann nur einer dieser Trustpoints, die die CA teilen, zur Validierung von Benutzerzertifikaten verwendet werden.

Konfiguration

Um über einen Remote-Client eine Verbindung zur ASA herzustellen, geben Sie in das Adressfeld eines SSL-fähigen Webbrowsers https://ASA_outside_address ein. ASA_outside_address ist die externe IP-Adresse Ihrer ASA. Wenn Ihre Konfiguration erfolgreich war, wird das Fenster Cisco Systems SSL VPN Client angezeigt.

Hinweis: Das Fenster Cisco Systems SSL VPN Client wird nur angezeigt, nachdem Sie das Zertifikat von der ASA akzeptiert haben und nachdem der SSL VPN Client auf die Remote-Station heruntergeladen wurde. Wenn das Fenster nicht angezeigt wird, stellen Sie sicher, dass es nicht minimiert ist.

Befehle

Mit WebVPN sind mehrere Befehle zum Anzeigen verknüpft. Sie können diese Befehle über die Kommandozeile ausführen, um Statistiken und andere Informationen anzuzeigen. Weitere Informationen zu show-Befehlen finden Sie unter Überprüfen von WebVPN-Konfigurationen.

Hinweis: Das Output Interpreter Tool (nur für registrierte Kunden) (OIT) unterstützt bestimmte show-Befehle. Verwenden Sie das OIT, um eine Analyse der show-Befehlsausgabe anzuzeigen.

Fehlerbehebung

Verwenden Sie diesen Abschnitt, um Probleme mit Ihrer Konfiguration zu beheben.

SVC-Fehler

Problem

Diese Fehlermeldung wird möglicherweise bei der Authentifizierung angezeigt:

```
"The SSl VPN connection to the remote peer was disrupted
and could not be automatically re-estabilished. A new connection requires
re-authentication and must be restarted manually. Close all sensitive networked
applications."
```

Lösung

Wenn ein Firewall-Dienst auf Ihrem PC ausgeführt wird, kann dies die Authentifizierung unterbrechen. Beenden Sie den Dienst, und stellen Sie die Verbindung zum Client wieder her.

Hat der SVC eine sichere Sitzung mit der ASA eingerichtet?

So stellen Sie sicher, dass der SSL VPN-Client eine sichere Sitzung mit der ASA hergestellt hat:

1. Klicken Sie auf Überwachung.
2. Erweitern Sie VPN Statistics, und wählen Sie Sessions aus.
3. Wählen Sie im Dropdown-Menü Filter By (Filtern nach) die Option SSL VPN Client aus, und klicken Sie auf die Schaltfläche Filter.

   Ihre Konfiguration sollte in der Sitzungsliste angezeigt werden.

Werden sichere Sitzungen eingerichtet und erfolgreich beendet?

Sie können die Echtzeitprotokolle anzeigen, um sicherzustellen, dass Sitzungen eingerichtet und erfolgreich beendet werden. Sitzungsprotokolle anzeigen:

1. Klicken Sie auf Überwachung und dann auf Protokollierung.
2. Wählen Sie die Echtzeit-Protokollanzeige oder den Protokollpuffer aus, und klicken Sie dann auf Anzeigen.

   Hinweis: Um nur Sitzungen einer bestimmten Adresse anzuzeigen, filtern Sie nach Adresse.

Überprüfen Sie den IP-Pool im WebVPN-Profil.

```
%ASA-3-722020: Group group User user-name IP IP_address  No address
available for SVC connection
```

Es sind keine Adressen verfügbar, die der SVC-Verbindung zugewiesen werden können. Weisen Sie daher die IP-Pool-Adresse im Profil zu.

Wenn Sie das neue Verbindungsprofil erstellen, konfigurieren Sie einen Alias oder eine Gruppen-URL, um auf dieses Verbindungsprofil zuzugreifen. Wenn nicht, werden alle SSL-Versuche das Standard-WebVPN-Verbindungsprofil treffen, an das kein IP-Pool gebunden war. Legen Sie diese Option fest, um das Standard-Verbindungsprofil zu verwenden und einen IP-Pool darauf zu speichern.

Tipps

- Stellen Sie sicher, dass das Routing mit dem IP-Adresspool, den Sie den Remote-Clients zuweisen, ordnungsgemäß funktioniert. Dieser IP-Adresspool sollte von einem Subnetz in Ihrem LAN stammen. Sie können auch einen DHCP-Server oder einen Authentifizierungsserver verwenden, um IP-Adressen zuzuweisen.
- Die ASA erstellt eine Standard-Tunnelgruppe (DefaultWebVPNGroup) und eine Standard-Gruppenrichtlinie (GroupPolicy1). Wenn Sie neue Gruppen und Richtlinien erstellen, stellen Sie sicher, dass Sie die Werte in Übereinstimmung mit den Sicherheitsrichtlinien Ihres Netzwerks anwenden.
- Wenn Sie das Durchsuchen von Windows-Dateien über CIFS aktivieren möchten, geben Sie einen WINS (NBNS)-Server unter Konfiguration > VPN > WebVPN > Server und URLs ein. Diese Technologie verwendet die CIFS-Auswahl.

Befehle

Mit WebVPN sind mehrere Debug-Befehle verknüpft. Ausführliche Informationen zu diesen

Befehlen finden Sie unter Verwenden von WebVPN-Debugbefehlen.

Hinweis: Die Verwendung von Debug-Befehlen kann sich negativ auf das Cisco Gerät auswirken. Lesen Sie den Artikel Important Information on Debug Commands (Wichtige Informationen zu Debug-Befehlen), bevor Sie debug-Befehle verwenden.

Zugehörige Informationen

- Clientless SSL VPN (WebVPN) auf ASA - Konfigurationsbeispiel
- Thin-Client SSL VPN (WebVPN) auf ASA mit ASDM - Konfigurationsbeispiel
- ASA mit WebVPN und einmaliger Anmeldung unter Verwendung von ASDM und NTLMv1 - Konfigurationsbeispiel
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Technischer Support und Dokumentation für Cisco Systeme

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.