ASA 8.x: Konfigurationsbeispiel für den VPN-Zugriff mit dem AnyConnect VPN-Client mithilfe eines selbstsignierten Zertifikats

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie selbstsignierte Zertifikate verwenden, um über den Cisco AnyConnect 2.0-Client SSL-VPN-Verbindungen mit der ASA für den Remote-Zugriff zuzulassen.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundlegende ASA-Konfiguration mit Softwareversion 8.0
- ASDM 6.0(2)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA 8.0(2), ASDM 6.0 (2)
- Cisco AnyConnect 2.0

Konventionen

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

Hintergrundinformationen

Der Cisco AnyConnect 2.0-Client ist ein SSL-basierter VPN-Client. Der AnyConnect-Client kann auf verschiedenen Betriebssystemen wie Windows 2000, XP, Vista, Linux (Mehrere Distributoren) und MAC OS X verwendet und installiert werden. Der AnyConnect-Client kann vom Systemadministrator manuell auf dem Remote-PC installiert werden. Sie kann auch auf die Sicherheits-Appliance geladen und für Remote-Benutzer zum Download bereit gestellt werden. Nachdem die Anwendung heruntergeladen wurde, kann sie sich nach dem Beenden der Verbindung automatisch selbst deinstallieren oder auf dem Remote-PC für zukünftige SSL VPN-Verbindungen verbleiben. In diesem Beispiel ist der AnyConnect-Client nach erfolgreicher browserbasierter SSL-Authentifizierung zum Download bereit.

Weitere Informationen zum AnyConnect 2.0-Client finden Sie in den Versionshinweisen zu AnyConnect 2.0.

Hinweis: MS Terminal Services wird nicht in Verbindung mit dem AnyConnect-Client unterstützt. Sie können kein RDP zu einem Computer erstellen und dann eine AnyConnect-Sitzung starten. Sie können kein RDP mit einem Client verbinden, der über AnyConnect verbunden ist.

Hinweis: Bei der ersten Installation von AnyConnect muss der Benutzer über Administratorrechte verfügen (unabhängig davon, ob Sie das eigenständige AnyConnect msi-Paket verwenden oder die pkg-Datei von der ASA übertragen). Wenn der Benutzer über keine Administratorrechte verfügt, wird ein Dialogfeld mit dieser Anforderung angezeigt. Bei nachfolgenden Upgrades muss der Benutzer, der AnyConnect zuvor installiert hat, keine Administratorrechte besitzen.

Konfigurieren

Gehen Sie wie folgt vor, um die ASA für den VPN-Zugriff mithilfe des AnyConnect-Clients zu konfigurieren:

1. Konfigurieren eines selbst ausgestellten Zertifikats.
2. Laden Sie das SSL VPN-Client-Image hoch, und identifizieren Sie es.
3. Aktivieren Sie AnyConnect Access.

4. Erstellen einer neuen Gruppenrichtlinie.
5. Konfigurieren der Umgehung von Zugriffslisten für VPN-Verbindungen.
6. Erstellen Sie ein Verbindungsprofil und eine Tunnelgruppe für die AnyConnect-Clientverbindungen.
7. Konfigurieren der NAT-Ausnahme für AnyConnect-Clients.
8. Hinzufügen von Benutzern zur lokalen Datenbank.

Schritt 1: Konfigurieren eines selbst ausgestellten Zertifikats

Standardmäßig verfügt die Sicherheits-Appliance über ein selbstsigniertes Zertifikat, das bei jedem Neustart des Geräts neu generiert wird. Sie können Ihr eigenes Zertifikat von Anbietern wie Verisign oder EnTrust erwerben oder die ASA so konfigurieren, dass sie sich selbst ein Identitätszertifikat ausstellt. Dieses Zertifikat bleibt auch beim Neustart des Geräts gleich. Führen Sie diesen Schritt aus, um ein selbst ausgestelltes Zertifikat zu generieren, das beim Neustart des Geräts erhalten bleibt.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Remotezugriffs-VPN**.
2. Erweitern Sie **Zertifikatsverwaltung**, und wählen Sie **Identitätszertifikate aus**.
3. Klicken Sie auf **Hinzufügen** und anschließend auf das Optionsfeld **Neues Identitätszertifikat hinzufügen**.
4. Klicken Sie auf **Neu**.
5. Klicken Sie im Dialogfeld Schlüsselpaar hinzufügen auf das Optionsfeld **Geben Sie den neuen Schlüsselpaarnamen ein**.
6. Geben Sie einen Namen ein, um die Tastatur zu identifizieren.In diesem Beispiel wird *sslvpnkeypair* verwendet.
7. Klicken Sie auf **Jetzt generieren**.
8. Stellen Sie sicher, dass im Dialogfeld Identitätszertifikat hinzufügen das neu erstellte Schlüsselpaar ausgewählt ist.
9. Geben Sie als ZertifikatSubject DN den vollqualifizierten Domänennamen (FQDN) ein, der für die Verbindung mit der VPN-Terminierungsschnittstelle verwendet wird.**CN=sslvpn.cisco.com**
10. Klicken Sie auf **Erweitert**, und geben Sie den FQDN ein, der für das Feld ZertifikatSubject DN verwendet wird.Beispiel: **FQDN**: sslvpn.cisco.com
11. Klicken Sie auf **OK**.
12. Aktivieren Sie das Kontrollkästchen **Selbst signiertes Zertifikat generieren**, und klicken Sie auf **Zertifikat hinzufügen**.
13. Klicken Sie auf **OK**.
14. Klicken Sie auf **Konfiguration** und dann auf **Remotezugriffs-VPN**.
15. Erweitern Sie **Erweitert**, und wählen Sie **SSL Settings** aus.
16. Wählen Sie im Zertifikatsbereich die Schnittstelle aus, die zum Beenden des SSL VPN (außerhalb) verwendet wird, und klicken Sie auf **Bearbeiten**.
17. Wählen Sie in der Dropdownliste Zertifikat das selbstsignierte Zertifikat aus, das Sie zuvor generiert haben.
18. Klicken Sie auf **OK** und dann auf **Übernehmen**.

Befehlszeilenbeispiel

Ciscoasa

```
ciscoasa(config)#crypto key generate rsa label
sslvpnkeypair
INFO: The name for the keys will be: sslvpnkeypair
Keypair generation process begin. Please wait...
!--- Generate an RSA key for the certificate. (The name
should be unique. !--- For example, sslvpnkeypair.)
ciscoasa(config)#crypto ca trustpoint localtrust
!--- Create a trustpoint for the self-issued
certificate. ciscoasa(config-ca-trustpoint)#enrollment
self
ciscoasa(config-ca-trustpoint)#fqdn sslvpn.cisco.com
ciscoasa(config-ca-trustpoint)#subject-name
CN=sslvpn.cisco.com
!--- The fully qualified domain name is used for both
fqdn and CN. !--- The name should resolve to the ASA
outside interface IP address. ciscoasa(config-ca-
trustpoint)#keypair sslvpnkeypair
!--- The RSA key is assigned to the trustpoint for
certificate creation. ciscoasa(config-ca-
trustpoint)#crypto ca enroll localtrust noconfirm
% The fully-qualified domain name in the certificate
will be: sslvpn.cisco.com
ciscoasa(config)# ssl trust-point localtrust outside
!--- Assign the trustpoint to be used for SSL
connections on the outside interface.
```

Schritt 2: Laden und Identifizieren des SSL VPN-Client-Image

In diesem Dokument wird der AnyConnect SSL 2.0-Client verwendet. Sie können diesen Client auf der Cisco Software Download-Website herunterladen. Für jedes Betriebssystem, das Remote-Benutzer verwenden möchten, ist ein separates AnyConnect-Image erforderlich. Weitere Informationen finden Sie in den Versionshinweisen zu Cisco AnyConnect 2.0.

Führen Sie nach Erhalt des AnyConnect-Clients die folgenden Schritte aus:

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Remotezugriffs-VPN**.
2. Erweitern Sie **Network (Client) Access**, und erweitern Sie dann **Advanced**.
3. Erweitern Sie **SSL VPN**, und wählen Sie **Client Settings** aus.
4. Klicken Sie im Bereich SSL VPN Client Images (Bilder des SSL VPN-Clients) auf **Add (Hinzufügen)** und dann auf **Upload (Hochladen)**.
5. Navigieren Sie zu dem Speicherort, an dem Sie den AnyConnect-Client heruntergeladen haben.
6. Wählen Sie die Datei aus, und klicken Sie auf **Datei hochladen**.Sobald der Client hochgeladen wurde, erhalten Sie eine Meldung, dass die Datei erfolgreich in den Flash-Speicher hochgeladen wurde.
7. Klicken Sie auf **OK**.Ein Dialogfeld wird angezeigt, um zu bestätigen, dass Sie das neu hochgeladene Image als aktuelles SSL VPN-Client-Image verwenden möchten.
8. Klicken Sie auf **OK**.
9. Klicken Sie auf **OK** und dann auf **Übernehmen**.
10. Wiederholen Sie die Schritte in diesem Abschnitt für jedes Betriebssystemspezifische

AnyConnect-Paket, das Sie verwenden möchten.

Befehlszeilenbeispiel

Ciscoasa

```
ciscoasa(config)#copy tftp://192.168.50.5/anyconnect-
win-2.0.0343-k9.pkg flash

Address or name of remote host [192.168.50.5]?

Source filename [anyconnect-win-2.0.0343-k9.pkg]?

Destination filename [anyconnect-win-2.0.0343-k9.pkg]?

Accessing tftp://192.168.50.5/anyconnect-win-2.0.0343-
k9.pkg...!!!!!!!!!!!!!
Writing file disk0:/anyconnect-win-2.0.0343-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
2635734 bytes copied in 4.480 secs (658933 bytes/sec)
!--- AnyConnect image is downloaded to ASA via TFTP.
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-
2.0.0343-k9.pkg 1
!--- Specify the AnyConnect image to be downloaded by
users. The image that is !--- downloaded the most should
have the lowest number. This image uses 1 for the !---
AnyConnect Windows image.
```

Schritt 3: AnyConnect-Zugriff aktivieren

Damit der AnyConnect-Client eine Verbindung zur ASA herstellen kann, müssen Sie den Zugriff auf die Schnittstelle aktivieren, die SSL VPN-Verbindungen terminiert. In diesem Beispiel wird die externe Schnittstelle verwendet, um AnyConnect-Verbindungen zu beenden.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Remotezugriffs-VPN**.
2. Erweitern Sie **den Netzwerkzugriff (Client)**, und wählen Sie dann **SSL VPN-Verbindungsprofile aus**.
3. Aktivieren Sie das Kontrollkästchen **Cisco AnyConnect VPN Client aktivieren**.
4. Aktivieren Sie das Kontrollkästchen **Zugriff zulassen** für die externe Schnittstelle, und klicken Sie auf **Übernehmen**.

Befehlszeilenbeispiel

Ciscoasa

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#svc enable
!--- Enable AnyConnect to be downloaded to remote
computers.
```

Schritt 4: Erstellen einer neuen Gruppenrichtlinie

Eine Gruppenrichtlinie legt die Konfigurationsparameter fest, die bei der Verbindung auf Clients angewendet werden sollen. In diesem Beispiel wird eine Gruppenrichtlinie mit dem Namen *SSLClientPolicy* erstellt.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Remotezugriffs-VPN**.
2. Erweitern Sie den **Netzwerkzugriff (Client)**, und wählen Sie **Gruppenrichtlinien aus**.
3. Klicken Sie auf **Hinzufügen**.
4. Wählen Sie **Allgemein**, und geben Sie **SSLClientPolicy** im Feld Name ein.
5. Deaktivieren Sie das Kontrollkästchen **Adresspools vererben**.
6. Klicken Sie auf **Auswählen** und dann auf **Hinzufügen**.Das Dialogfeld "IP-Pool hinzufügen" wird angezeigt.
7. Konfigurieren Sie den Adresspool aus einem IP-Bereich, der derzeit in Ihrem Netzwerk nicht verwendet wird.In diesem Beispiel werden folgende Werte verwendet:**Name**: SSLClientPool**Start-IP-Adresse**: 192.168.25.1**End IP-Adresse**: 192.168.25.50**Subnetzmaske**: 255.255.255,0
8. Klicken Sie auf **OK**.
9. Wählen Sie den neu erstellten Pool aus, und klicken Sie auf **Zuweisen**.
10. Klicken Sie auf **OK** und dann auf **Weitere Optionen**.
11. Deaktivieren Sie das Kontrollkästchen **Tunneling Protocols Inherit** (Tunneling-Protokolle erben).
12. Aktivieren Sie **SSL VPN Client**.
13. Wählen Sie im linken Teilfenster **Server** aus.
14. Deaktivieren Sie das Kontrollkästchen "DNS Servers **Inherit**", und geben Sie die IP-Adresse des internen DNS-Servers ein, den die AnyConnect-Clients verwenden werden.In diesem Beispiel wird *192.168.50.5* verwendet.
15. Klicken Sie auf **Weitere Optionen**.
16. Deaktivieren Sie das Kontrollkästchen Default Domain **Inherit** (Standarddomänenvererbung).
17. Geben Sie die von Ihrem internen Netzwerk verwendete Domäne ein. Beispielsweise *tsweb.local*.
18. Klicken Sie auf **OK** und dann auf **Übernehmen**.

Befehlszeilenbeispiel

Ciscoasa

```
ciscoasa(config)#ip local pool SSLClientPool
192.168.25.1-192.168.25.50 mask 255.255.255.0
!--- Define the IP pool. The IP pool should be a range
of IP addresses !--- not already in use on the internal
network. ciscoasa(config)#group-policy SSLCLientPolicy
internal
ciscoasa(config)#group-policy SSLCLientPolicy attributes
ciscoasa(config-group-policy)#dns-server value
192.168.50.5
!--- Specify the internal DNS server to be used.
ciscoasa(config-group-policy)#vpn-tunnel-protocol svc
!--- Specify VPN tunnel protocol to be used by the Group
Policy. ciscoasa(config-group-policy)#default-domain
value tsweb.local
!--- Define the default domain assigned to VPN users.
```

```
ciscoasa(config-group-policy)#address-pools value
SSLClientPool
!--- Assign the IP pool created to the SSLClientPolicy
group policy.
```

Konfigurieren der Umgehung von Zugriffslisten für VPN-Verbindungen

Wenn Sie diese Option aktivieren, erlauben Sie den SSL/IPsec-Clients, die Liste der Schnittstellenzugriffe zu umgehen.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Remotezugriffs-VPN**.
2. Erweitern Sie **Network (Client) Access**, und erweitern Sie dann **Advanced**.
3. Erweitern Sie **SSL VPN**, und wählen Sie **Bypass Interface Access List (Schnittstellenzugriffsliste umgehen)**.
4. Stellen Sie sicher, dass das Kontrollkästchen **Eingehende SSL VPN- und IPSEC-Sitzungen aktivieren, um die Schnittstellenzugriffslisten zu umgehen** aktiviert ist, und klicken Sie auf **Übernehmen**.

Befehlszeilenbeispiel

Ciscoasa

```
ciscoasa(config)#sysopt connection permit-vpn
!--- Enable interface access-list bypass for VPN
connections. !--- This example uses the vpn-filter
command for access control.

ciscoasa(config-group-policy)#
```

Schritt 6: Erstellen eines Verbindungsprofils und einer Tunnelgruppe für die AnyConnect-Clientverbindungen

Wenn VPN-Clients eine Verbindung mit der ASA herstellen, stellen sie eine Verbindung zu einem Verbindungsprofil oder einer Tunnelgruppe her. Die Tunnelgruppe wird verwendet, um Verbindungsparameter für bestimmte VPN-Verbindungstypen zu definieren, z. B. IPsec L2L, IPsec-Remote-Zugriff, clientloses SSL und Client-SSL.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Remotezugriffs-VPN**.
2. Erweitern Sie **den Netzwerkzugriff (Client)**, und erweitern Sie dann **SSL VPN**.
3. Wählen Sie **Verbindungsprofile aus**, und klicken Sie auf **Hinzufügen**.
4. Wählen Sie **Basic (Grundlegend)**, und geben Sie die folgenden Werte ein:**Name**: SSLClientProfile**Authentifizierung**: LOKAL**Standardgruppenrichtlinie**: SSLClientPolicy
5. Stellen Sie sicher, dass das Kontrollkästchen **SSL VPN Client Protocol** aktiviert ist.
6. Erweitern Sie im linken Teilfenster die Option **Erweitert**, und wählen Sie **SSL VPN aus**.
7. Klicken Sie unter VerbindungsAliase auf **Hinzufügen**, und geben Sie einen Namen ein, dem Benutzer ihre VPN-Verbindungen zuordnen können. Beispiel: *SSLVPNClient*.
8. Klicken Sie auf **OK** und anschließend erneut auf **OK**.
9. Aktivieren Sie am unteren Rand des ASDM-Fensters das Kontrollkästchen **Allow user to**

select connection (Verbindung durch Alias in der Tabelle oben auf der Anmeldeseite zulassen), und klicken Sie auf **Apply**.

Befehlszeilenbeispiel

Ciscoasa

```
ciscoasa(config)#tunnel-group SSLClientProfile type
remote-access
!--- Define tunnel group to be used for VPN remote
access connections. ciscoasa(config)#tunnel-group
SSLClientProfile general-attributes
ciscoasa(config-tunnel-general)#default-group-policy
SSLCLientPolicy
ciscoasa(config-tunnel-general)#tunnel-group
SSLClientProfile webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias SSLVPNClient
enable
!--- Assign alias for tunnel group. ciscoasa(config-
tunnel-webvpn)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
!--- Enable alias/tunnel group selection for SSL VPN
connections.
```

Schritt 7: Konfigurieren der NAT-Ausnahme für AnyConnect-Clients

Die NAT-Ausnahme sollte für alle IP-Adressen oder IP-Bereiche konfiguriert werden, auf die die SSL VPN-Clients zugreifen können sollen. In diesem Beispiel benötigen die SSL VPN-Clients nur Zugriff auf die interne IP-Adresse 192.168.50.5.

Hinweis: Wenn NAT-Control nicht aktiviert ist, ist dieser Schritt nicht erforderlich. Überprüfen Sie mithilfe des Befehls **show run nat-control**. Klicken Sie zum Überprüfen über ASDM auf **Konfiguration**, **Firewall** und wählen Sie **NAT Rules aus**. Wenn das Kontrollkästchen **Datenverkehr durch die Firewall ohne Adressübersetzung aktivieren** aktiviert ist, können Sie diesen Schritt überspringen.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Firewall**.
2. Wählen Sie **NAT Rules** aus, und klicken Sie auf **Add**.
3. Wählen Sie **Add NAT Exempt Rule (NAT-Regel hinzufügen)**, und geben Sie die folgenden Werte ein:**Aktion**: Freistellung**Schnittstelle**: innen**Quelle**: 192.168,50,5**Ziel**: 192.168.25.0/24**NAT-Freistellungsrichtung**: NAT Ausgehender Datenverkehr von der Schnittstelle "inside" in niedrigere Sicherheitsschnittstellen ausweisen (Standard)
4. Klicken Sie auf **OK** und dann auf **Übernehmen**.

Befehlszeilenbeispiel

Ciscoasa

```
ciscoasa(config)#access-list no_nat extended permit
                 ip host 192.168.50.5 192.168.25.0
255.255.255.0
!--- Define access list to be used for NAT exemption.
ciscoasa(config)#nat (inside) 0 access-list no_nat
!--- Allow external connections to untranslated internal
```

```
!--- addresses defined by access lisy no_nat.
ciscoasa(config)#
```

Schritt 8: Hinzufügen von Benutzern zur lokalen Datenbank

Wenn Sie die lokale Authentifizierung (die Standardauthentifizierung) verwenden, müssen Sie Benutzernamen und Kennwörter in der lokalen Datenbank für die Benutzerauthentifizierung definieren.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Remotezugriffs-VPN**.
2. Erweitern Sie **AAA-Setup**, und wählen Sie **Lokale Benutzer** aus.
3. Klicken Sie auf **Hinzufügen**, und geben Sie die folgenden Werte ein:**Benutzername**: Matthewp**Kennwort**: p@ssw0rd**Kennwort bestätigen**: p@ssw0rd
4. Wählen Sie das Optionsfeld **Kein ASDM, SSH, Telnet oder Konsolenzugriff aus**.
5. Klicken Sie auf **OK** und dann auf **Übernehmen**.
6. Wiederholen Sie diesen Schritt für weitere Benutzer, und klicken Sie dann auf **Speichern**.

Befehlszeilenbeispiel

Ciscoasa

```
ciscoasa(config)#username matthewp password p@ssw0rd
ciscoasa(config)#username matthewp attributes
ciscoasa(config-username)#service-type remote-access
!--- Assign user remote access only. No SSH, Telnet,
ASDM access allowed. ciscoasa(config-username)#write
memory
!--- Save the configuration.
```

Überprüfen

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob die SSL VPN-Konfiguration erfolgreich ist.

Herstellen einer Verbindung zur ASA mit dem AnyConnect-Client

Installieren Sie den Client direkt auf einem PC, und stellen Sie eine Verbindung zur ASA-Außenschnittstelle her, oder geben Sie https und die FQDN/IP-Adresse der ASA in einen Webbrowser ein. Wenn Sie einen Webbrowser verwenden, installiert sich der Client nach erfolgreicher Anmeldung.

SSL VPN-Clientverbindungen überprüfen

Verwenden Sie den Befehl **show vpn-sessiondb svc**, um verbundene SSL VPN-Clients zu überprüfen.

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc

Session Type: SVC

Username     : matthewp              Index        : 6
```

```
Assigned IP  : 192.168.25.1           Public IP    : 172.18.12.111
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 35466                  Bytes Rx     : 27543
Group Policy : SSLClientPolicy        Tunnel Group : SSLClientProfile
Login Time   : 20:06:59 UTC Tue Oct 16 2007
Duration     : 0h:00m:12s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

ciscoasa(config-group-policy)#
```

Der **Befehl vpn-sessiondb logoff name *username* meldet Benutzer nach Benutzername ab.** Beim Trennen der Verbindung wird eine *Administrator Reset*-Meldung an den Benutzer gesendet.

```
ciscoasa(config)#vpn-sessiondb logoff name matthewp
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "matthewp" logged off : 1

ciscoasa(config)#
```

Weitere Informationen zum AnyConnect 2.0-Client finden Sie im Cisco AnyConnect VPN-Administratorhandbuch.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung (optional)

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug webvpn svc 255** - Zeigt Debugmeldungen über Verbindungen zu SSL VPN-Clients über WebVPN an.**Erfolgreiche AnyConnect-Anmeldung**

```
ciscoasa(config)#debug webvpn svc 255
INFO: debug webvpn svc enabled at level 255.
ciscoasa(config)#ATTR_FILTER_ID: Name:
 SSLVPNClientAccess
, Id: 1, refcnt: 1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.10.1.5' - !--- Outside IP of ASA Processing CSTP header line: 'Host:
10.10.1.5'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' - !--- AnyConnect Version
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' Setting
user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343' webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=3338474156@28672@1192565782@EFB9042D72C
63CE02164F790435897AC72EE70AE' Processing CSTP header line: 'Cookie:
webvpn=3338474156@28672@119 2565782@EFB9042D72C63CE02164F790435897AC72EE70AE' Found WebVPN
cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE'
```

```
WebVPN Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02
164F790435897AC72EE70AE' IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782'
webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header line:
'X-CSTP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field() ...input: 'X-
CSTP-Hostname: wkstation1' - !--- Client desktop hostname Processing CSTP header line: 'X-
CSTP-Hostname: wkstation1'
Setting hostname to: 'wkstation1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451CB0948AFBE98296FD849
                          49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
Processing CSTP header line: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451C
       B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:
                             DES-CBC3-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.25.1/255.255.255.0 - !--- IP assigned from IP Pool CSTP
state = HAVE_ADDRESS SVC: NP setup np_svc_create_session(0x7000, 0xD41612C8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED
webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
might not be enabled or invalid policy
```

AnyConnect-Anmeldung fehlgeschlagen (falsches Kennwort)

```
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_portal.c:http_webvpn_kill_cookie[627]
webvpn_auth.c:http_webvpn_pre_authentication[1905]
WebVPN: calling AAA with ewsContext (-717386088) and nh (-717388536)!
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[4380]
WebVPN: AAA status = (REJECT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_auth.c:http_webvpn_post_authentication[1180]
WebVPN: user: (matthewp) rejected.
http_remove_auth_handle(): handle 9 not found!
webvpn_portal.c:ewaFormServe_webvpn_login[1749]
webvpn_portal.c:http_webvpn_kill_cookie[627]
```

Zugehörige Informationen

- Administratoranleitung für den Cisco AnyConnect VPN Client, Version 2.0
- Versionshinweise für AnyConnect VPN Client, Version 2.0

- Technischer Support und Dokumentation - Cisco Systems