ASA 8.x: Split Tunneling für AnyConnect VPN-Client im ASA-Konfigurationsbeispiel zulassen

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Konfigurieren Netzwerkdiagramm ASA-Konfiguration mit ASDM 6.0(2) ASA CLI-Konfiguration Einrichtung der SSL VPN-Verbindung mit SVC Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument enthält schrittweise Anweisungen, wie Cisco AnyConnect VPN-Client-Zugriff auf das Internet ermöglicht wird, während sie in eine Cisco Adaptive Security Appliance (ASA) 8.0.2 getunnelt werden. Diese Konfiguration ermöglicht dem Client den sicheren Zugriff auf Unternehmensressourcen über SSL und bietet gleichzeitig ungesicherten Zugriff auf das Internet durch Split-Tunneling.

Voraussetzungen

Anforderungen

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

- ASA Security Appliance muss Version 8.x ausführen
- Cisco AnyConnect VPN Client 2.xHinweis: Laden Sie das AnyConnect VPN Client-Paket (anyconnect-win*.pkg) vom Cisco <u>Software Download herunter</u> (nur registrierte Kunden). Kopieren Sie den AnyConnect VPN-Client in den Flash-Speicher der ASA, der auf die Computer der Remote-Benutzer heruntergeladen werden soll, um die SSL VPN-Verbindung mit der ASA herzustellen. Weitere Informationen finden Sie im Abschnitt <u>Installation des</u> <u>AnyConnect Client</u> im ASA-Konfigurationsleitfaden.

Verwendete Komponenten

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

- Cisco ASA der Serie 5500 mit Softwareversion 8.0(2)
- Cisco AnyConnect SSL VPN Client-Version für Windows 2.0.0343
- PC mit Microsoft Vista, Windows XP SP2 oder Windows 2000 Professional SP4 und Microsoft Installer Version 3.1
- Cisco Adaptive Security Device Manager (ASDM) Version 6.0(2)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Der Cisco AnyConnect VPN Client stellt sichere SSL-Verbindungen zur Sicherheits-Appliance für Remote-Benutzer bereit. Ohne einen zuvor installierten Client geben Remote-Benutzer die IP-Adresse einer Schnittstelle in ihrem Browser ein, die für die Annahme von SSL VPN-Verbindungen konfiguriert ist. Wenn die Sicherheits-Appliance nicht so konfiguriert ist, dass http:// Anfragen an https:// umgeleitet werden, müssen Benutzer die URL im Formular https://<address> eingeben.

Nach der Eingabe der URL stellt der Browser eine Verbindung zu dieser Schnittstelle her und zeigt den Anmeldebildschirm an. Wenn der Benutzer die Anmeldung und Authentifizierung erfüllt und die Sicherheits-Appliance den Benutzer als den Client erfordert, lädt sie den Client herunter, der dem Betriebssystem des Remote-Computers entspricht. Nach dem Herunterladen installiert und konfiguriert sich der Client selbst, stellt eine sichere SSL-Verbindung her und bleibt bzw. deinstalliert sich beim Beenden der Verbindung (abhängig von der Konfiguration der Sicherheits-Appliance) selbst.

Bei einem bereits installierten Client überprüft die Sicherheits-Appliance bei der Benutzerauthentifizierung die Client-Version und aktualisiert den Client bei Bedarf.

Wenn der Client eine SSL VPN-Verbindung mit der Security Appliance aushandelt, wird die Verbindung über Transport Layer Security (TLS) und optional über Datagram Transport Layer Security (DTLS) hergestellt. DTLS vermeidet Latenz- und Bandbreitenprobleme im Zusammenhang mit einigen SSL-Verbindungen und verbessert die Leistung von Echtzeitanwendungen, die empfindlich auf Paketverzögerungen reagieren.

Der AnyConnect-Client kann von der Sicherheits-Appliance heruntergeladen oder vom Systemadministrator manuell auf dem Remote-PC installiert werden. Weitere Informationen zur manuellen Installation des Clients finden Sie im <u>Administratorhandbuch</u> für den Cisco AnyConnect VPN Client. Die Sicherheits-Appliance lädt den Client basierend auf den Gruppenrichtlinien- oder Benutzernamen-Attributen des Benutzers, der die Verbindung herstellt, herunter. Sie können die Sicherheitsappliance so konfigurieren, dass der Client automatisch heruntergeladen wird, oder Sie können sie so konfigurieren, dass der Remote-Benutzer aufgefordert wird, den Client herunterzuladen. Im letzteren Fall, wenn der Benutzer nicht antwortet, können Sie die Sicherheits-Appliance so konfigurieren, dass der Client entweder nach einer Timeout-Periode heruntergeladen wird oder die Anmeldeseite angezeigt wird.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind <u>RFC 1918</u> -Adressen, die in einer Laborumgebung verwendet werden.

ASA-Konfiguration mit ASDM 6.0(2)

In diesem Dokument wird davon ausgegangen, dass die Basiskonfiguration, z. B. die Schnittstellenkonfiguration, bereits erstellt wurde und ordnungsgemäß funktioniert.

Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter <u>Zulassen von</u> <u>HTTPS-Zugriff für ASDM</u>.

Hinweis: WebVPN und ASDM können nicht auf derselben ASA-Schnittstelle aktiviert werden, es sei denn, Sie ändern die Portnummern. Weitere Informationen finden Sie unter <u>ASDM und</u>

WebVPN Enabled auf derselben ASA-Schnittstelle.

Gehen Sie wie folgt vor, um das SSL VPN auf ASA mit Split-Tunneling zu konfigurieren:

1. Wählen Sie Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add aus, um einen IP-Adresspool vpnpool zu

| 8 | 🗟 Add IP Pool | | |
|------------|--------------------|-----------------|------|
| | | | |
| | Name: | vpnpool | |
| | Starting IP Addres | ss: 192.168.10. | 1 |
| | Ending IP Addres | s: 192.168.10. | 254 |
| | Subnet Mask: | 255.255.255 | .0 |
| | | | |
| erstellen. | ок | Cancel | Help |

- 2. Klicken Sie auf Übernehmen.Entsprechende CLI-Konfiguration:
- 3. Aktivieren Sie WebVPN.Wählen Sie Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles aus, und klicken Sie unter Access Interfaces auf die Kontrollkästchen Allow Access and Enable DTLS for the external interface. Aktivieren Sie außerdem das Kontrollkästchen Enable Cisco AnyConnect VPN Client or Legacy SSL VPN Client access (Cisco AnyConnect VPN-Client oder Legacy-SSL VPN-Client-Zugriff aktivieren) in der in der Tabelle unten ausgewählten Schnittstelle, um SSL VPN auf der externen Schnittstelle zu aktivieren.

| Configuration > Rem | ote Access VPN > Net | work (Client) Access > SSL VPM | I Connection Profiles | |
|---|--|--------------------------------------|---------------------------|--|
| The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options. | | | | |
| (More client-related | (More client-related parameters, such as client images and client profiles, can be found at <u>Client Settings</u> | | | |
| | | | | |
| 🔽 Enable Cisco Any | Connect VPN Client or le | egacy SSL VPN Client access on the i | nterfaces selected in the | |
| Interface | Allow Access | Require Client Certificate | Enable DTLS | |
| outside | | | | |
| inside | | | | |
| Access Darks 442 | DTLC Davis | | | |
| Access Port: 443 | DILS Port: | 443 | | |
| Click here to Assign | Certificate to Interface. | | | |

Klicken Sie auf Übernehmen.Wählen Sie Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add, um das Cisco AnyConnect VPN-Client-Image aus dem Flash-Speicher der ASA hinzuzufügen, wie gezeigt.

| Flash SVC Image: Upload Upload untered operation system to the top of the OK Cancel Help Correct Help Folders Files Files Oryzałow o | Add SSL VPN Client Image SSL VPN > Client Settings | | | |
|--|--|----------------------------------|------------------|------------------------------|
| Upload untered operation system to the top of the OK Cancel Help Polders Files Folders Files Image: Crypto_archive 07/24/07 05:21:48 Image: Ct-win-2.0.0343-k9.pkg 07/13/07 04:16:30 Image: Ct-win-2.0.0343-k9.pkg 07/13/07 04:16:30 Image: Ct-win-2.0.0343-k9.pkg 07/13/07 04:16:30 | Flash SVC Image: | Browse Flash | 2 | |
| OK Cancel Help Folders Files Image: Crypto_archive 07/24/07 05:21:48 Image: Crypto_archive 07/24/07 05:21:36 asdm=603.bin 6,651,212 Image: Crypto_archive 07/24/07 05:21:36 asdm=603.bin 6,651,212 Image: Crypto_archive 07/24/07 05:21:36 asdm=602.bin 6,859,764 Image: Crypto_archive 0.2635,734 Image: Crypto_archive 0.2635,734 Image: Crypto_archive 0.2009/20/07 09:51:38 asdm=602.bin 6,869,764 0.1/03/08 21:39:26 asa802+48.bin 14,524,416 0.1/03/08 21:39:26 asa802+48.bin 14,524,416 0.01/03/08 21:39:26 asa802+48.bin 14,524,416 0.01/03/08 21:39:26 asa802+48.bin 14,524,416 0.01/03/08 21:39:26 asa802+48.bin 14,524,416 0.01/03/08 21:39:26 asa802+48.bin 14,824,416 0.01/03/08 21:39:26 asa802+48.bin 14,824,416 0.01/03/08 21:39:26 Bill Marketter Bill Marketter Bill Marketeeeeeeeeeee | | Upload | buntered operati | ion system to the top of the |
| Folders Files Image: Constraint of the second | ОК | Cancel Help | | |
| Es browse rrash Files Folders Files File Gistor Grypto_archive 07/24/07 05:21:48 Grypto_archive 07/24/07 05:21:49 Grypto_archive 07/24/07 05:21:40 Grypto_archive 1,635,008 Grypto_archive 1,635,008 Grypto_archive 1,635,008 Grypto_archive 1,220 Grypto_archive 6,889,764 Grypto_archive 6,8312,832 Grypto_archive 1,41,524,416 Grypto_archive 1,841 Grypto_archive 1,841 Gryp | | | | |
| Folders Files FileName Size (bytes) Date Modified Grypto_archive 07/24/07 05:21:48 07/24/07 05:21:48 Glog 07/24/07 05:21:48 07/24/07 05:21:48 Glog 07/24/07 05:21:48 07/24/07 05:21:38 asdm-603.bin 6,851,212 01/04/08 18:07:02 ass803:48.bin 14,635,008 01/04/08 17:49:50 admin.cfg 1,220 09/20/07 09:51:38 arryconnect-win-2.0.03 2,635,734 08/13/07 04:14:50 asdm-602.bin 6,889,764 01/03/08 21:38:26 asa722:48.bin 8,312,832 02/13/07 04:16:30 asdm-522.bin 5,623,108 02/12/07 09:51:38 asa802:48.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 asslclent-win-2.0.0343-k9.pkg Erewse Flash Flash 5VC Image: Flash 5VC Image: ct-win-2.0.0343-k9.pkg Erowse Flash Upload OK Cancel Help Klicken Sie auf OK. OK Cancel Help | prowse riasn | | | ^ |
| FileName Size (bytes) Date Modified Ing 0rypto_archive 07/24/07 05:21:48 07/24/07 05:21:48 Ing 0rypto_archive 07/24/07 05:1:48 07/24/07 05:1:48 Ing 1,220 09/20/07 09:51:38 09/20/07 09:51:38 Ing asdm-602.bin 6,889,764 01/03/08 21:38:26 Ing asdm-522.bin 5,623,108 02/12/07 05:53:48 Ing asdm-522.bin 14,524,416 01/03/08 21:24:42 Ing_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 Ing Add SSL VPN Client Image Ing Ing Ing Ing Add SSL VPN Client Image Upload Uplo | Folders | Files | | |
| Image: Crypto_archive O7/24/07 05:21:48 Image: Crypto_archive 0g 07/24/07 05:21:36 asdm-603.bin 6,851,212 01/04/08 18:07:02 asdm-603.bin 14,635,008 01/04/08 17:49:50 admin.cfg 1,220 09/20/07 09:51:38 arryconnect-win-2.0.03 2,635,734 08/13/07 04:14:50 asdm-602.bin 6,889,764 01/03/08 21:38:26 asdm-522.bin 5,623,108 02/12/07 05:53:48 asa602-k8.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 ass602-k8.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 asslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg Erowse Flash Upload Upload Upload OK Cancel Help Klicken Sie | 🖃 🥪 disk0: | FileName 🔬 | Size (bytes) | Date Modified |
| Image: Crypto_archive Image: Crypto_archive 07/24/07 05:21:36 asdm-603.bin 6,851,212 01/04/08 18:07:02 asa803-k8.bin 14,635,008 01/04/08 17:49:50 admin.cfg 1,220 09/20/07 09:51:38 anyconnect-win-2:0.03 2,635,734 08/13/07 04:14:50 asdm-602.bin 6,889,764 01/03/08 21:38:26 asar-602.bin 6,889,764 01/03/08 21:38:26 asar-522.bin 5,623,108 02/12/07 05:53:48 asdm-522.bin 5,623,108 02/12/07 09:51:38 asdm-522.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg Browse Flash Upload Upload Upload Klicken Sie auf OK. Ct-win-2.0.0343-k9.pkg Klicken Sie auf OK. | | Crypto_archive | | 07/24/07 05:21:48 |
| asdm-603.bin 6,851,212 01/04/08 18:07:02 asa803-k8.bin 14,635,008 01/04/08 17:49:50 admin.cfg 1,220 09/20/07 09:51:38 anyconnect-win-2.0.03 2,635,734 08/13/07 04:14:50 asam-602.bin 6,889,764 01/03/08 21:38:26 asam-602.bin 6,889,764 01/03/08 21:38:26 asam-522.bin 5,623,108 02/12/07 09:53:48 asabu-522.bin 5,623,108 02/12/07 09:51:38 asabu-522.bin 5,623,108 02/12/07 09:51:38 asabu-522.bin 5,623,108 02/12/07 09:51:38 asabu-522.bin 5,623,108 02/12/07 09:51:38 asabu-522.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg Enowse Flash Upload Upload Upload OK Cancel Help Klicken Sie auf OK Cancel Help | | 🛄 log | | 07/24/07 05:21:36 |
| asa803-k8.bin 14,635,008 01/04/08 17:49:50 admin.cfg 1,220 09/20/07 09:51:38 admodelect-win-2,0,03 2,635,734 08/13/07 04:14:50 asdm-602.bin 6,889,764 01/03/08 21:38:26 asa722-k8.bin 8,312,832 02/13/07 04:16:30 asdm-522.bin 5,623,108 02/12/07 05:53:48 asa802-k8.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg Flash SVC Image: Ct-win-2,0.0343-k9.pkg Browse Flash Upload Upload OK Klicken Sie auf OK. | | asdm-603.bin | 6,851,212 | 01/04/08 18:07:02 |
| admin.cfg 1,220 09/20/07 09:51:38 anyconnect-win-2,0,03 2,635,734 08/13/07 04:14:50 asdm-602.bin 6,889,764 01/03/08 21:38:26 asa722-k8.bin 8,312,832 02/13/07 04:16:30 asdm-522.bin 5,623,108 02/12/07 05:53:48 asa802-k8.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg File Name: anyconnect-win-2.0.0343-k9.pkg File Name: Ct-win-2.0.0343-k9.pkg Filesh SVC Image: Ct-win-2,0.0343-k9.pkg Klicken Sie auf OK. Klicken Sie auf OK. | | asa803-k8.bin | 14,635,008 | 01/04/08 17:49:50 |
| anyconnect-win-2.0.03 2,635,734 08/13/07 04:14:50 asdm-602.bin 6,889,764 01/03/08 21:38:26 asa722-k8.bin 8,312,832 02/13/07 04:16:30 asdm-522.bin 5,623,108 02/12/07 05:53:48 asa802-k8.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg File Name: anyconnect-win-2.0.0343-k9.pkg File Name: anyconnect-win-2.0.0343-k9.pkg Klicken Sie auf OK. OK Cancel Help Klicken Sie auf OK. | | admin.cfg | 1,220 | 09/20/07 09:51:38 |
| asdm-602,bin 6,889,764 01/03/08 21:38:26 asa722+k8,bin 8,312,832 02/13/07 04:16:30 asdm-522,bin 5,623,108 02/12/07 05:53:48 asa802+k8,bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg File Name: Add SSL VPN Client Image Flash SVC Image: ct-win-2.0.0343-k9.pkg Browse Flash Upload OK Cancel Help Klicken Sie auf OK. OK Cancel Help | | anyconnect-win-2.0.03 | 2,635,734 | 08/13/07 04:14:50 |
| asa722-k8.bin 8,312,832 02/13/07 04:16:30 asdm-522.bin 5,623,108 02/12/07 05:53:48 asa802-k8.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg Files Name: ct-win-2.0.0343-k9.pkg Browse Flash Upload OK Ct-win-2.0.0343-k9.pkg Klicken Sie auf OK. Klicken Sie auf OK. | | asdm-602.bin | 6,889,764 | 01/03/08 21:38:26 |
| asdm-522.bin 5,623,108 02/12/07 05:53:48 asa802-k8.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg File Name: anyconnect-win-2.0.0343-k9.pkg File Name: Ct-win-2.0.0343-k9.pkg Browse Flash Upload OK Cancel Help Klicken Sie auf OK. Add S5L VPN Client Image Ct-win-2.0.0343-k9.pkg Browse Flash Upload OK Cancel Help Klicken Sie auf OK. | | asa722-k8.bin | 8,312,832 | 02/13/07 04:16:30 |
| asa802-k8.bin 14,524,416 01/03/08 21:24:42 old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg File Name: anyconnect-win-2.0.0343-k9.pkg File Name: Ct-win-2.0.0343-k9.pkg Browse Flash Upload Klicken Sie auf OK. Cancel Help Klicken Sie auf OK. | | asdm-522.bin | 5,623,108 | 02/12/07 05:53:48 |
| old_running.cfg 1,841 09/20/07 09:51:38 sslclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg File Name: anyconnect-win-2.0.0343-k9.pkg File Name: ct-win-2.0.0343-k9.pkg File Name: OK Cancel Help Klicken Sie auf OK. OK Cancel Help Klicken Sie auf OK. | | asa802-k8.bin | 14,524,416 | 01/03/08 21:24:42 |
| ssiclient-win-1.1.4.179 418,765 03/14/08 13:47:58 File Name: anyconnect-win-2.0.0343-k9.pkg File Name: anyconnect-win-2.0.0343-k9.pkg Flash 5VC Image: ct-win-2.0.0343-k9.pkg Browsee Flash Upload Klicken Sie auf OK. OK Cancel Help Klicken Sie auf OK. Klicken Sie Klicken Sie | | old_running.cfg | 1,841 | 09/20/07 09:51:38 |
| File Name: anyconnect-win-2.0.0343-k9.pkg File Name: anyconnect-win-2.0.0343-k9.pkg Flash SVC Image: ct-win-2.0.0343-k9.pkg Browse Flash Upload Upload OK Cancel Help Klicken Sie auf OK. Klicken Sie | | sslclient-win-1.1.4.179 | 418,765 | 03/14/08 13:47:58 |
| File Name: anyconnect-win-2.0.0343-k9.pkg Image: Add SSL VPN Client Image Flash SVC Image: ct-win-2.0.0343-k9.pkg Browse Flash Upload Upload OK Cancel Help Klicken Sie auf OK. Klicken Sie | | | | |
| Klicken Sie auf OK. OK Cancel Help Klicken Sie auf OK. Klicken Sie auf Klicken Sie | File Na | me: anyconnect-win-2.0.0343-k9.p | kg | |
| Flash SVC Image: ct-win-2.0.0343-k9.pkg Browse Flash Upload Upload Klicken Sie auf OK. Cancel Help Klicken Sie auf Klicken Sie | (c) | Add SSL VPN Client Image | | : |
| Flash SVC Image: ct-win-2.0.0343-k9.pkg Browse Flash Upload OK Cancel Help Klicken Sie auf OK. Klicken Sie auf Klicken Sie | | | | |
| Upload OK Cancel Help Klicken Sie auf OK. | Fla | sh SVC Image: ct-win-2.0.0343 | -k9.pkg Browse | e Flash |
| Klicken Sie auf OK Cancel Help Klicken Sie auf | | | Upl | oad |
| auf | Klicken Sie auf OK | OK Canc | el Help | Klicken Sic |
| | auf | | | |
| Hinzufügen. | Hinzufügen. | | | |

| Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings | | |
|--|--|--|
| Identify SSL VPN Client (SVC) related files. | | |
| SSL VPN Client Images | | |
| Minimize connection setup time by moving the image used by the most commonly encountered operation system to t | | |
| 🛧 Add 🗹 Replace 🛱 Delete 🛧 Move UP 🗲 Move Down | | |
| disk0:/anvconnect-win-2.0.0343-k9.pkg | | |

Entsprechende CLI-Konfiguration:

4. Konfigurieren Sie die Gruppenrichtlinie.Wählen Sie Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remote Access VPN > Netzwerk (Client) Access > Group Policies (Konfigurationsrichtlinien), um eine interne Gruppenrichtlinien-Clientgruppe zu erstellen. Aktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen SSL VPN Client, um das WebVPN als Tunneling-Protokoll zu aktivieren

| | Add Internal Group Policy | |
|-----|---------------------------|--|
| | | |
| - [| General) | Name: (clientgroup) |
| | Servers | |
| | -Advanced | Banner: 🔽 Inherit |
| | -Split Tunneling | |
| | -IE Browser Proxy | Address Pools: 🔽 Inherit |
| | SSL VPN Client | |
| | | More Options |
| | | The options |
| | | Tunneling Protocols: 🔽 Inherit 🔽 Clientless SSL VPN 🔽 SSL VPN Client 🔽 IPsec |

Deaktivieren Sie auf der Registerkarte **Erweitert > Getrenntes Tunneling** das Kontrollkästchen **Erben** für Split Tunnel Policy (Tunnel-Richtlinie teilen), und wählen Sie **unten** in der Dropdown-Liste die Option **Tunnel Network List (Tunnel-Netzwerkliste)** aus.



Deaktivieren Sie das Kontrollkästchen Erben für die Split Tunnel Network List (Kanalliste für Tunnel-Netzwerk teilen), und klicken Sie dann auf Manage (Verwalten), um den ACL

Manager zu

| 🚰 Edit Internal Group Policy: | hivalleyvpn |
|--|--|
| General Servers Advanced E Browser Proxy SSL VPN Client SSL VPN Client Free Client Client Access Rule Client Firewall Hardware Client | Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network. DNS Names: Inherit Policy: Inherit Tunnel Network List Below Network List: Inherit None Inherit I |

Wählen Sie im ACL Manager **Hinzufügen > ACL hinzufügen aus..** um eine neue Zugriffsliste zu



Geben Sie einen Namen für die ACL an, und klicken Sie auf

| UK. | | | | |
|------------------------|-----------------|---------------|-------------|--|
| 🔂 ACL Manag | jer | | | |
| Standard A | CL Extended ACL | | | |
| 🔂 Add 🚽 | Edit 📋 Delete | ታ ፋ ሯ ፝ 🖻 🕮 | * | |
| No | Address | Action | Description | |
| 🔂 Add A | CL | | X | |
| ACL Name: split-tunnel | | | | |
| | OK Can | cel Hel | o | |

Sobald der ACL-Name erstellt wurde, wählen Sie Add > Add ACE (Hinzufügen > ACE hinzufügen, um einen Zugriffssteuerungseintrag (ACE) hinzuzufügen.Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das Netzwerk 10.77.241.128/26 und wählen Zulassen als Aktion aus.Klicken Sie auf OK, um den ACL Manager zu verlassen.

| No | Address | Action | Desc | ription |
|--------------|-------------------|--------|------|---------|
| split-tunnel | | | | |
| 付 Add ACE | | | | |
| Host/Netw | ork | | | |
| IP Addre | ss: 10.77.241.128 | | | • |
| Netmask | : 255.255.255.192 | | | • |
| Description: | | | | |
| Beschption. | | | | |

Stellen Sie sicher, dass die gerade erstellte ACL für die Split-Tunnel-Netzwerkliste ausgewählt ist. Klicken Sie auf **OK**, um zur Gruppenrichtlinienkonfiguration zurückzukehren.

| 🔂 Add Internal Group Policy | | | | | | × |
|---|---|--|---|---|------------------------------------|-----------------------------------|
| General Servers Advanced <u>Splt Tunneling</u> IE Browser Proxy E-SSL VPN Client E-IPsec Client | Split tunneling networequire tunneling. Th ACL that consists of DNS Names: 🔽 Init Policy: 🔲 Init | rk lists distinguish ne le security appliance list of addresses on I herit herit | tworks that require makes split tunnelin the private network. | traffic to go through the g decisions on the basis o | tunnel and tho f a network list | ise that do not t, which is an |
| | Network List: 🥅 Ini | herit split-tunnel | | | | Manage |
| | Intercept DHCP | Configuration Me | ssage from Micos | oft Clients | | ۲ |

Klicken Sie auf der Hauptseite auf **Übernehmen** und dann auf Senden (falls erforderlich), um die Befehle an die ASA zu senden.Konfigurieren Sie die **SSL VPN-**Einstellungen im Gruppenrichtlinienmodus.Deaktivieren Sie für die Option Installer auf Client-System beibehalten das Kontrollkästchen **Erben**, und klicken Sie auf das Optionsfeld **Ja**.Dadurch kann die SVC-Software auf dem Client-Rechner 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.

| 🚘 Edit Internal Group Policy: clientgroup | | | | |
|---|----------------------------------|-----------|-----------|-----------|
| General | Keep Installer on Client System: | 🔲 Inherit | • Yes | C No |
| -Servers | Compression: | 🔽 Inherit | C Enable | C Disab |
| | Datagram TLS: | 🔽 Inherit | C Enable | C Disab |
| Login Setting | Keepalive Messages: | 🔽 Inherit | 🗖 Disable | Interval: |

Klicken Sie auf Login Setting, um die Post Login-Einstellung und die Post Login-Standardauswahl wie dargestellt

| festzul | egen |
|---------|------|
|---------|------|

| 10 | solzuleyen. | |
|----|--------------------------------|---|
| | General | After successfully logging in, user can have the choice to download the client software, or g |
| | Servers | portal page. The following securitys decides what will happen. |
| | E-Advanced | 🔲 Inherit |
| | -Split Tunneling | |
| | IE Browser Proxy | Post Login Setting |
| | -SSL VPN Client -Login Setting | Do not prompt user to choose |
| | Key Regeneration | C Prompt user to choose |
| | | User has seconds to choose, or Default Post Login Selection below is take |
| | ⊡—IPsec Client | |
| | | Default Post Login Selection |
| | | C Go to Clientless SSL VPN portal |
| | | Download SSL VPN Client |

Deaktivieren Sie bei der Option zum Intervall der Neuverhandlung das Kontrollkästchen **Erben**, deaktivieren Sie das Kontrollkästchen **Unlimited (Unbegrenzt)**, und geben Sie die Anzahl der Minuten bis zum erneuten Auftreten ein.Die Sicherheit wird verbessert, indem die Gültigkeitsdauer eines Schlüssels beschränkt wird.Deaktivieren Sie für die Option Methode der Neuverhandlung das Kontrollkästchen **Erben**, und klicken Sie auf das **SSL-**Optionsfeld.Bei der Neuverhandlung kann der aktuelle SSL-Tunnel oder ein neuer Tunnel verwendet werden, der speziell für die Neuverhandlung erstellt wurde.

| | Renegotiation Interval: | 🔲 Inherit | 🔲 Unlimited | 30 | minutes |
|-----------------------------------|-------------------------|-----------|-------------|-------|--------------|
| E-Advanced | Renegotiation Method: | 🔲 Inherit | O None | ⊙ SSL | C New Tunnel |
| —Split Tunneling | | | | | |
| -IE Browser Proxy | | | | | |
| 🖨 SSL VPN Client | | | | | |
| Login Setting Key Regeneration |) | | | | |

Klicken Sie auf **OK** und dann auf **Übernehmen**.

| Co | nfiguration > Remote Access VPN > | • Net | work (Client) Access | • Group Policies |) | |
|-----|--|-----------------|---|---|--|----------------------|
| | Manage VPN group policies. A VPN grou externally on a RADIUS/LDAP server. T | p poli he gr | cy is a collection of user-c oup policy information is r | riented attribute/va eferenced by VPN tu | lue pairs that may be sto innel groups and user acc | red inter :ounts. |
| | 🔂 Add 🔻 🗹 Edit 📋 Delete | | | | | |
| | Name | | Туре | Tunne | ling Protocol | |
| - (| clientgroup |) | Internal | svc | | N/A - |
| | DfltGrpPolicy (System Default) | | Internal | L2TP-IPSec, IPSec, v | vebvpn | N/A - |

Entsprechende CLI-Konfiguration:

5. Wählen Sie **Configuration > Remote Access VPN > AAA Setup > Local Users > Add** aus, um ein neues Benutzerkonto **ssluser1** zu erstellen. Klicken Sie auf **OK** und dann auf

| Übernehmen. | |
|---------------------------------------|---|
| 🔄 Add User Account | |
| <mark>Identity</mark> ⊕-VPN Policy | Username: ssluser1 Password: ****** Confirm Password: ****** User authenticated using MSCHAP |
| | Member-of |
| | Member-of: Add >> Delete |
| | Select and of the entirest below to verticit ASDM_SSH_Telept and Concele access |
| | Select one of the options below to restrict ASDM, SSR, Teinet and Console access. |
| | Note: All users have network access, regardless of these settings. |
| | Full access(ASDM, SSH, Telnet and Console) |
| | Privilege level is used with command authorization. |
| | Privilege Level: 2 |
| | CLI login prompt for SSH, Telnet and console (no ASDM access) |
| | This setting is effective only if AAA authenticate console command is configured. |
| | O No ASDM, SSH, Telnet or Console access |
| | This setting is effective only if AAA authenticate console command is configured. |

Entsprechende CLI-Konfiguration:

6. Wählen Sie Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit aus, um die Standardservergruppe LOCAL zu ändern, indem Sie das Kontrollkästchen Enable Local User Lockout (Lokale Benutzersperre aktivieren) mit dem Wert für maximale Zugriffsversuche auf 16 aktivieren.

| Configurati | ion > Remote | Access VPN > AA | A Setup > AAA Server | Groups | |
|-------------|---|--|---|--|---|
| AAA Serve | er Groups — | | | | |
| Ser | ver Group | Protocol | Accounting Mode | Reactivation Mode | |
| LOCAL | | LOCAL | | | |
| | Edit LOCA This feature before lockin when the loc Enable Loc Maximum | Allows you to speci g out and denying al database is used ocal User Lockout Attempts: 16 | fy the maximum number of access to the user. This I for authentication. | of failed attempts to allov imit is applicable only Help | × |

- 7. Klicken Sie auf OK und dann auf Übernehmen Entsprechende CLI-Konfiguration:
- 8. Konfigurieren Sie die Tunnelgruppe.Wählen Sie Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles Profile > Add, um eine neue Tunnelgruppen-SSL-Gruppe zu erstellen.Auf der Registerkarte Basic (Grundlegende) können Sie die folgende Konfigurationsliste ausführen:Geben Sie der Tunnelgruppe den Namen sslgroup.Wählen Sie unter Client Address Assignment (Client-Adressenzuweisung) den Adresspool vpnpool aus der Dropdown-Liste aus.Wählen Sie unter Default Group Policy (Standardgruppenrichtlinie) die Gruppenrichtlinien-Clientgruppe aus der Dropdown-Liste

| aus. | | | _ |
|--------------------------|------------------------|---------------------------------|--------|
| 👰 Add SSL VPN Connection | n Profile | | |
| Basic R-Advanced | Name: | ssigroup | |
| | Aliases: | | |
| | Authentication —— | | |
| | Method: | ⊙ AAA C Certificate C Both | |
| | AAA Server Group: | LOCAL | Manag |
| | | Use LOCAL if Server Group fails | |
| | Client Address Assign | nent | |
| | DHCP Servers: | | |
| | Client Address Pools: | vpnpool | Select |
| | Default Group Policy | | |
| | Group Policy: | clientgroup | Manag |
| | SSL VPN Client Protoco | | |
| | OK | Cancel Help | |

Geben Sie auf der Registerkarte SSL VPN > Connection Aliases (SSL VPN >

VerbindungsAliase) den Namen des Gruppen-Alias als **sslgroup_users** an, und klicken Sie auf _____

| Basic | Portal Page Customization: DfltCustomization |
|--|---|
| Advanced General Client Addressing Authentication Authorization Accounting SSL VPN | CSD Alternate Group Policy: DfltGrpPolicy CSD Alternate display of Radius Reject-Message on th Connection Aliases Add Collecte |
| | ✓ Add Connection Alias Alias: sslgroup_users ✓ Enabled OK Cancel Help |
| | 🔂 Add 📓 Delete |

n Sie auf OK und dann auf Übernehmen Entsprechende CLI-Konfiguration:

9. Konfigurieren Sie NAT.Wählen Sie Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule (Konfiguration > Firewall > NAT-Regeln > Dynamische NAT-Regel hinzufügen, damit der Datenverkehr aus dem internen Netzwerk mit der externen IP-Adresse 172.16.1.5 übersetzt werden

| s 🖻 | Add Dynamic | NAT Rule | |
|------|-----------------|-------------------------------|-------------------------------------|
| Or | riginal — | | |
| | Interface: insi | de | V |
| | Source: any | / | |
| - | | | |
| Ir | anslated — | | |
| | Select a global | pool for dynamic translation. | |
| | Pool ID | Interface | Addresses Pool |
| | 0 | (outbound) | Same as original address (identity) |
| | -0 | (inbound) | Same as original address (identity) |
| | 1 | outside | 🖳 172.16.1.5 |
| 111. | | | |

cken Sie auf **OK**.Klicken Sie auf **OK**.

| ¢ | Configura | tion > Firewall > NA | AT Rules | | | | |
|---|------------|----------------------|------------|-------------|-------------|--------------------|-----|
| | 🔂 Add | 🝷 📝 Edit 🗻 De | lete 🕈 🗲 👗 | 🖻 💼 🛛 🔍 | Find 🔛 Diag | gram 🛛 🟹 Packet Tr | ace |
| l | # | Tupa | | Original | | | |
| l | * | туре | Source | Destination | Service | Interface | |
| I | 🗆 inside (| (1 Dynamic rules) | | | | | |
| | 1 | 🙀 Dynamic | 🌍 any | | | outside | |

Klicken Sie auf Übernehmen. Entsprechende CLI-Konfiguration:

10. Konfigurieren Sie die NAT-Ausnahme für den Rückverkehr vom internen Netzwerk zum VPN-Client.

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
```

```
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0
```

ciscoasa(config)#nat (inside) 0 access-list nonat

ASA CLI-Konfiguration

| Cisco ASA 8.0(2) |
|--|
| |
| ciscoasa(config)# show running-config |
| : Saved |
| : |
| ASA Version 8.0(2) |
| |
| nostname ciscoasa |
| aomain-name default.domain.invalid |
| names |
| 1 |
| interface Ethernet0/0 |
| nameif inside |
| security-level 100 |
| ip address 10.77.241.142 255.255.255.192 |
| ! |
| interface Ethernet0/1 |
| nameif outside |
| security-level 0 |
| ip address 172.16.1.1 255.255.255.0 |
| |
| interface Ethernet0/2 |
| shutdown |
| no nameli |
| no security-ievel |
| |
| interface Ethernet0/3 |
| shutdown |
| no nameif |
| no security-level |
| no ip address |
| ! |
| interface Management0/0 |
| shutdown |
| no nameif |
| no security-level |
| no ip address |
| |
| passwa 2KFQnbNldl.2KYOU encrypted |

boot system disk0:/asa802-k8.bin ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid access-list split-tunnel standard permit 10.77.241.128 255.255.255.192 !--- ACL for Split Tunnel network list for encryption. access-list nonat permit ip 10.77.241.0 192.168.10.0 access-list nonat permit ip 192.168.10.0 10.77.241.0 !--- ACL to define the traffic to be exempted from NAT. pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 !--- The address pool for the Cisco AnyConnect SSL VPN Clients no failover icmp unreachable rate-limit 1 burstsize 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 global (outside) 1 172.16.1.5 !--- The global address for Internet access used by VPN Clients. !--- Note: Uses an RFC 1918 range for lab setup. !--- Apply an address from your public range provided by your ISP. nat (inside) 0 access-list nonat !--- The traffic permitted in "nonat" ACL is exempted from NAT. nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list class-map inspection_default match default-inspection-traffic 1 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 netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp service-policy global_policy global webvpn enable outside !--- Enable WebVPN on the outside interface svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1 !--- Assign an order to the AnyConnect SSL VPN Client image svc enable !--- Enable the security appliance to download SVC images to remote computers tunnel-group-list enable !--- Enable the display of the tunnel-group list on the WebVPN Login page group-policy clientgroup internal !--- Create an internal group policy "clientgroup" group-policy clientgroup attributes vpn-tunnel-protocol svc !--- Specify SSL as a permitted VPN tunneling protocol split-tunnel-policy tunnelspecified split-tunnel-network-list value split-tunnel !--- Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed !--- When the security appliance and the SVC perform a rekey, they renegotiate !--- the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 !--- Command that specifies the number of minutes from the start of the !--- session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl !--- Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted !--- Create a user account "ssluser1" tunnel-group sslgroup type remote-access !--- Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool !--- Associate the address pool vpnpool created defaultgroup-policy clientgroup

!--- Associate the group policy "clientgroup" created



Einrichtung der SSL VPN-Verbindung mit SVC

Gehen Sie wie folgt vor, um eine SSL VPN-Verbindung mit ASA herzustellen:

1. Geben Sie die URL oder die IP-Adresse der WebVPN-Schnittstelle der ASA in Ihrem Webbrowser im gezeigten Format ein.

| nttps://uri |
|--|
| ODER |
| https:// <ip address="" asa="" interface="" of="" the="" webvpn=""></ip> |
| WEDVPN Service - Microsoft Internet Explorer |
| File Edit View Favorites Tools Help |
| 🌀 Back 🔹 🕑 🕤 📓 🐔 🔎 Search 🤺 Favorites 🤣 🎯 - 🌺 🔜 🦓 |
| Address an https://172.16.1.1/+webvpn+/index.html |
| CISCO SYSTEMS will live WebVPN Service |
| |
| Login |
| Please enter your username and password. |
| USERNAME: |
| PASSWORD: |
| GROUP: sslgroup_users |
| Login Clear |

2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Wählen Sie auch Ihre jeweilige Gruppe aus der Dropdown-Liste aus, wie

| | Login |
|-------------------|--------------------------|
| Please enter your | r username and password. |
| USERNAME: | ssluser1 |
| PASSWORD: | •••••• |
| GROUP: | sslgroup_users 🔽 |
| + | Login Clear |

dargestellt.

Fenster wird angezeigt, bevor die SSL VPN-Verbindung hergestellt

| wira |
|------|
| |



inweis: Die ActiveX-Software muss auf Ihrem Computer installiert sein, bevor Sie den SVC herunterladen können. Sie erhalten dieses Fenster, sobald die Verbindung hergestellt ist.



3. Klicken Sie auf die Sperre, die in der Taskleiste Ihres Computers angezeigt

| 🔌 Connection | 🚯 Statistics 🙈 About | | |
|--------------|----------------------|---|--|
| | cisco | | |
| Connect to: | 172.16.1.1 | ~ | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | Disconnect | | |

angezeigt und enthält Informationen zur SSL-Verbindung. Beispielsweise ist **192.168.10.1** die zugewiesene IP von der ASA

| Cisco AnyConnect VPN C | lient 🔳 🗖 |
|------------------------------------|----------------------------|
| 🔌 Connection 🕕 Statistics | 읅 About |
| cisc | I I O |
| Tunnel State: | Connected |
| Client Address: Server Address: | 192.168.10.1 172.16.1.1 |
| Bytes Sent: | 23461 |
| Bytes Received: | 1111 |
| Time Connected: | 00:04:51 |
| Details | |
| VPN session established. | |

In diesem Fenster werden

die Versionsinformationen des Cisco AnyConnect VPN-Clients



- - -

<u>Überprüfen</u>

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

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

 show webvpn svc: Zeigt die im ASA-Flash-Speicher gespeicherten SVC-Images an. ciscoasa#show webvpn svc
 disk0:/anyconnect-win-2.0.0343-k9.pkg 1

```
CISCO STC win2k+
2,0,0343
Mon 04/23/2007 4:16:34.63
```

- 1 SSL VPN Client(s) installed
- show vpn-sessiondb svc: Zeigt Informationen über die aktuellen SSL-Verbindungen an. ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username : **ssluser1**

| Assigned IP | : | 192.168.10.1 | Public IP | : | 192.168.1.1 |
|--------------|---|-------------------------|----------------|----|--------------------------------|
| Protocol | : | Clientless SSL-Tunnel | DTLS-Tunnel | | |
| Encryption | : | RC4 AES128 | Hashing | : | SHA1 |
| Bytes Tx | : | 194118 | Bytes Rx | : | 197448 |
| Group Policy | : | clientgroup | Tunnel Group | : | sslgroup |
| Login Time | : | 17:12:23 IST Mon Mar 2 | 24 2008 | | |
| Duration | : | 0h:12m:00s | | | |
| NAC Result | : | Unknown | | | |
| VLAN Mapping | : | N/A | VLAN | : | none |
| abovy waby | _ | aroun alian Zaiat dan I | configurierten | ٨١ | iaa für varachiadana Crunnan a |

- show webvpn group-alias: Zeigt den konfigurierten Alias für verschiedene Gruppen an.
 - Tunnel Group: sslgroup Group Alias: sslgroup_users enabled
- Wählen Sie im ASDM Monitoring > VPN > VPN Statistics > Sessions aus, um die aktuellen WebVPN-Sitzungen in der ASA zu

| e | fahren. | | | | | | | | |
|---|--|--------------|--|-----------------|--------------------------------|------------------------|------------------|-------------------|------|
| 6 | onitoring > VP | 'N > VPN S | tatistic | s > Sessions |) | | | | |
| Г | Sessions | | | | | | | | |
| | Remote | | Cito (| SSL VPN | | | E mail Drawn | VDN Load Palancia | |
| | Access | Site-to-Site | | Clientless | With Client | Total | E-mail Proxy | VPN LOad balancin | ן פי |
| | 0 0 | | | 0 | 0 | 0 | 0 | 0 | |
| | Filter By: SSL | VPN Client | | All Sessions | - • | | Fil | ter | |
| | Username Group Policy IP Address Connection | | | Proto Encryp | col Ition | Login Time Duration | | Byl | |
| | ssluser1 clientgroup 192.168.10.1 sslgroup | | Clientless SSL-Tunnel DT RC4 AES128 | | 17:12:23 IST Mon 0h:03m:31s | Mar 24 2008 | 194118 192474 | | |

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

1. vpn-sessiondb logoff name *<username>*: Befehl zum Abmelden der SSL VPN-Sitzung für den jeweiligen Benutzernamen.

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1
ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)
```

Ebenso können Sie den Befehl **vpn-sessiondb logoff svc** verwenden, um alle SVC-Sitzungen zu beenden.

2. **Hinweis:** Wenn der PC in den Standby- oder Ruhemodus wechselt, kann die SSL VPN-Verbindung beendet werden.

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e
tc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
```

ciscoasa#**show vpn-sessiondb svc** INFO: There are presently no active sessions

 debug webvpn svc <1-255>: Stellt die Webvpn-Ereignisse in Echtzeit bereit, um die Sitzung einzurichten.

Ciscoasa#debug webvpn svc 7

```
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: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
... input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
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=16885952@12288@1206098825@D251883E8625B92C1338D631B08B
7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
625B92C1338D631B08B7D75F4EDEF26 '
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B
08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7
5F4EDEF26'
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: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
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: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40
642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
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: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask ... must calculate it
```

| SVC: NP setup |
|--|
| <pre>np_svc_create_session(0x3000, 0xD41611E8, TRUE)</pre> |
| webvpn_svc_np_setup |
| SVC ACL Name: NULL |
| SVC ACL ID: -1 |
| SVC ACL ID: -1 |
| <pre>vpn_put_uauth success!</pre> |
| 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 |

4. Wählen Sie im ASDM Monitoring > Logging > Real-time Log Viewer > View (Überwachung > Anmeldung > Echtzeit-Protokollanzeige > Anzeigen), um die Ereignisse in Echtzeit anzuzeigen.

| 🔂 Cisco ASDM 6.0 for ASA - 10.77.241.142 | | | | | | | |
|--|---|-------------------|----------------------------------|---|---|--|--|
| File | <u>View T</u> ools Wi <u>z</u> ards <u>Wi</u> | ndow <u>H</u> elp | | Look For: | _ | | |
| | Home 🦓 Configuration [|] Monitoring | 🔚 Save 🔇 Refresh 🔇 Ba | ack 🕥 Forward 💡 Help | | | |
| | Logging 🗖 | φ× ι | Monitoring > Logging > Real-Time | e Log Viewer | | | |
| e List | Real-Time Log Viewer | | Real-Time Log Viewer | | | | |
| Devic | Log Butter | | | | | | |
| | | | Click the View button belo | w to start displaying syslog messages in real time. Select th | e | | |
| | | | desired logging level to se | ee messages at that severity or higher. | | | |
| | | | | | | | |
| | | | Logging Level: | Debugging 💌 | | | |
| | | | | | | | |
| | | | | | | | |
| | | | Buffer Limit: | 1000 | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | View | | | |
| | | | | | | | |

Dieses Beispiel zeigt, dass die SSL-Sitzung mit dem Headend-Gerät eingerichtet wurde.

| 💑 Real-Time Log Viewer - 10.77.241.142 | | | | | | | | | |
|--|-------------|----------|-----------|--------------|----------------|--|--|--|--|
| <u>Fie Tools Window Help</u> | | | | | | | | | |
| 🕕 Pause 🖻 Copy 🎧 Save 🎝 Clear 📅 Color Settings 🏠 Create Rule 🛃 Show Rule 🔞 Show Details 🦿 Help | | | | | | | | | |
| Filter By: Filter I Show All Find: | | | | | | | | | |
| Severity | Date | Time | Syslog ID | Source IP | Destination IP | | | | |
| <u>4</u> 6 | Mar 21 2008 | 20:03:36 | 725007 | 10.77.233.74 | | SSL session with dient inside:10.77.233.74/1026 terminated. | | | |
| <u>4</u> 6 | Mar 21 2008 | 20:03:35 | 106015 | 10.77.233.74 | 10.77.241.142 | Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44 | | | |
| <u>4</u> 6 | Mar 21 2008 | 20:03:35 | 302014 | 10.77.233.74 | 10.77.241.142 | Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identii | | | |
| <u>4</u> 6 | Mar 21 2008 | 20:03:35 | 605005 | 0.0.0.0 | 0.0.0.0 | Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enable | | | |
| A 6 | Mar 21 2008 | 20:03:35 | 725002 | 10.77.233.74 | | Device completed SSL handshake with client inside:10.77.233.74/1026 | | | |
| <u>4</u> 6 | Mar 21 2008 | 20:03:35 | 725003 | 10.77.233.74 | | SSL client inside:10.77.233.74/1026 request to resume previous session. | | | |
| A 6 | Mar 21 2008 | 20:03:35 | 725001 | 10.77.233.74 | | Starting SSL handshake with client inside: 10.77.233.74/1026 for TLSv1 se | | | |
| <u>4</u> 6 | Mar 21 2008 | 20:03:35 | 302013 | 10.77.233.74 | 10.77.241.142 | Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23 | | | |
| | | | | | | | | | |
| ASA-6 725002 Device completed SSL handshake with remote_device interface_name:IP_address/port The SSL handshake has completed successfully with the remote device. | | | | | | | | | |

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliances der Serie 5500
- Versionshinweise für AnyConnect VPN Client, Version 2.0
- ASA/PIX: Split Tunneling für VPN-Clients im ASA-Konfigurationsbeispiel zulassen
- <u>Router ermöglicht VPN-Clients die Verbindung von IPsec und Internet mithilfe des Split</u> <u>Tunneling-Konfigurationsbeispiels</u>
- Beispiel für eine Stick-Konfiguration: PIX/ASA 7.x und VPN-Client für Public Internet VPN
- SSL VPN Client (SVC) auf ASA mit ASDM Konfigurationsbeispiel
- <u>Technischer Support und Dokumentation Cisco Systems</u>