ASA: Remote-Access-VPN im Multi-Context-Modus (AnyConnect)

Einführung

In diesem Dokument wird beschrieben, wie Remote Access (RA) Virtual Private Network (VPN) auf der Cisco Adaptive Security Appliance (ASA)-Firewall im MC-Modus mithilfe der CLI konfiguriert wird. Es zeigt die von der Cisco ASA unterstützten/nicht unterstützten Funktionen im Multiple-Context-Modus sowie die Lizenzierungsanforderungen in Bezug auf RA VPN.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ASA AnyConnect SSL-Konfiguration
- ASA Konfiguration mehrerer Kontexte

Verwendete Komponenten

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

- AnyConnect Secure Mobility Client Version 4.4.00243
- Zwei ASA5525 mit ASA Software Version 9.6(2)

Hinweis: Laden Sie das AnyConnect VPN Client-Paket vom Cisco Software Download herunter (nur registrierte Kunden).

Hinweis: 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.

Hintergrundinformationen

Multi-Context ist eine Form der Virtualisierung, bei der mehrere unabhängige Kopien einer Anwendung gleichzeitig auf derselben Hardware ausgeführt werden können, wobei jede Kopie (bzw. jedes virtuelle Gerät) für den Benutzer als separates physisches Gerät erscheint. So kann eine einzelne ASA mehreren unabhängigen Benutzern als mehrere ASAs angezeigt werden. Die ASA-Produktfamilie unterstützt seit ihrer ersten Version virtuelle Firewalls. Remote Access wurde in der ASA jedoch nicht für die Virtualisierung unterstützt. Für die Version 9.0 wurde die Unterstützung von VPN LAN2LAN (L2L) für Multi-Context hinzugefügt.

Hinweis: Von **9.5.2** Multi-Context-basierte Virtualisierungsunterstützung für VPN Remote Access (RA)-Verbindungen zur ASA

Ab **9.6.2** unterstützen wir die Flash-Virtualisierung, was bedeutet, dass wir AnyConnect-Image pro Kontext haben können.

Funktionsverlauf für Multikontext

Neue Funktionen in ASA 9.6(2) hinzugefügt

Funktion	Beschreibung
Vorbelegungs-/Benutzernamen-vom-Zertifikat-Funktion für mehrere Kontextmodi	Die AnyConnect SSL-Unterstützung wird erweitert, sodass CLIs für Vorfüll- und Benutzernamen aus Zertifikaten, die bisher nur im Einzelmodus verfügbar waren, auch im Multiple-Context-Modus aktiviert werden können.
Flash-Virtualisierung für Remote Access VPN	Remotezugriff-VPN im Multiple-Context-Modus unterstützt jetzt die Flash-Virtualisierung. Jeder Kontext kann einen privaten Speicherplatz und einen gemeinsam genutzten Speicherplatz auf der Basis des verfügbaren Flash-Gesamtwerts aufweisen.
Unterstützung von AnyConnect-Clientprofilen in Multi-Context-Geräten	AnyConnect-Clientprofile werden in Multi-Context-Geräten unterstützt. Um ein neues Profil mit ASDM hinzuzufügen, müssen Sie über den AnyConnect Secure Mobility Client Version 4.2.00748 oder 4.3.03013 und höher verfügen.
Stateful Failover für AnyConnect-Verbindungen im Multiple-Context-Modus	Stateful Failover wird jetzt für AnyConnect-Verbindungen im Multiple-Context-Modus unterstützt.
Remote Access VPN Dynamic Access Policy (DAP) wird im Multiple-Context-Modus unterstützt.	Sie können DAP jetzt pro Kontext im Multiple-Context-Modus konfigurieren.
Remote Access VPN CoA (Autorisationsänderung) wird im Multiple-Context-Modus unterstützt	Sie können CoA jetzt pro Kontext im Multiple-Context-Modus konfigurieren.
Remote Access VPN-Lokalisierung wird im Multiple-Context-Modus unterstützt	Lokalisierung wird global unterstützt. Es gibt nur einen Satz von Lokalisierungsdateien, die über verschiedene Kontexte hinweg gemeinsam genutzt werden.
Paketerfassungsspeicher pro Kontext wird unterstützt.	Diese Funktion ermöglicht es Benutzern, eine Erfassung direkt aus einem Kontext in den externen Speicher oder den privaten Kontext im Flash-Speicher zu kopieren. Diese Funktion ermöglicht auch das Kopieren der Roherfassung in die externen Paketerfassungstools, z. B. Wired-shark, innerhalb eines Kontexts.

Funktionen in ASA 9.5(2)

Funktion	Beschreibung
AnyConnect 4.x und höher (nur SSL VPN) keine IKEv2-Unterstützung)	Multi-Context-basierte Virtualisierungsunterstützung für VPN Remote Access (RA)-Verbindungen zur ASA.
Zentralisierte AnyConnect-Image-Konfiguration	• Flash-Speicher sind nicht virtualisiert. • Das AnyConnect-Image wird global im Admin-Kontext konfiguriert, und die Konfiguration gilt für alle Kontexte
Upgrade auf AnyConnect-Image	AnyConnect-Clientprofile werden in Multi-Context-Geräten unterstützt. Um ein neues Profil mit ASDM hinzuzufügen, müssen Sie über den AnyConnect Secure Mobility Client Version 4.2.00748 oder 4.3.03013 und höher verfügen.
Kontextressourcenmanagement für AnyConnect-Verbindungen	• Konfigurierbarkeit zur Kontrolle der maximalen Lizenznutzung pro Kontext • Konfigurierbarkeit für das Lizenz-Bursting pro Kontext

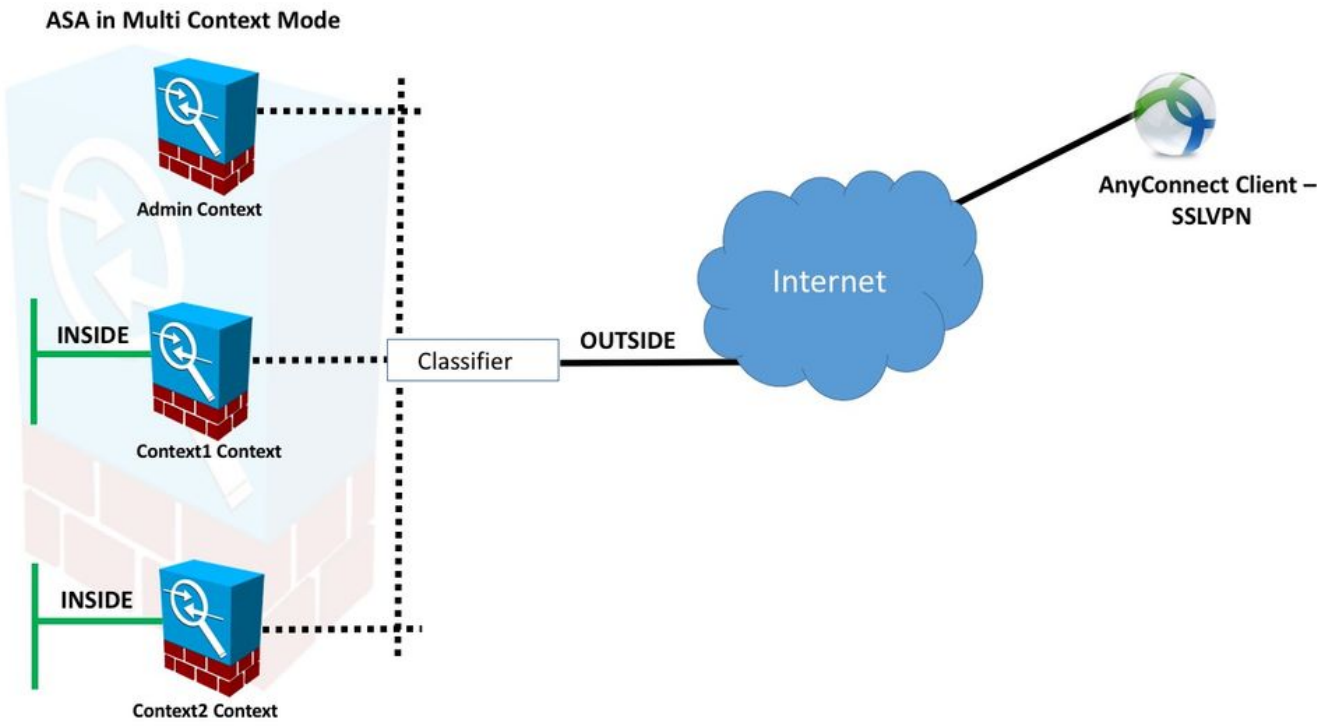
Lizenzierung

- AnyConnect Apex-Lizenz erforderlich
- Essentials-Lizenzen ignoriert/nicht zulässig
- Konfigurierbarkeit zur Kontrolle der maximalen Lizenznutzung pro Kontext
- Konfigurierbarkeit für das Lizenz-Bursting pro Kontext

Konfigurieren

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

Netzwerkdiagramm



Hinweis: Mehrere Kontexte in diesem Beispiel teilen eine Schnittstelle (OUTSIDE), dann verwendet der Klassifizierer die eindeutigen (automatischen oder manuellen) MAC-Adressen der Schnittstelle, um Pakete weiterzuleiten. Weitere Informationen zur Klassifizierung von Paketen in mehreren Kontext durch die Security Appliance finden Sie unter Wie die ASA Pakete klassifiziert

Das folgende Konfigurationsverfahren gilt für die ASA Version 9.6.2 und höher. Es zeigt einige der neuen verfügbaren Funktionen.Die Unterschiede im Konfigurationsverfahren für ASA-Versionen vor 9.6.2 (und höher 9.5.2) sind in Anhang A des Dokuments dokumentiert.

Nachfolgend werden die erforderlichen Konfigurationen im Systemkontext und in benutzerdefinierten Kontexten für die Einrichtung des Remote Access VPN beschrieben:

Erstkonfigurationen im Systemkontext

Zunächst konfigurieren Sie im Systemkontext Failover, VPN-Ressourcenzuweisung, benutzerdefinierte Kontexte und die Apex-Lizenzüberprüfung. Die Verfahren und Konfigurationen werden in diesem Abschnitt und im nächsten Abschnitt beschrieben.

Schritt 1: Failover-Konfiguration.

```
 !! Active Firewall

failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

```
 !! Secondary Firewall

failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

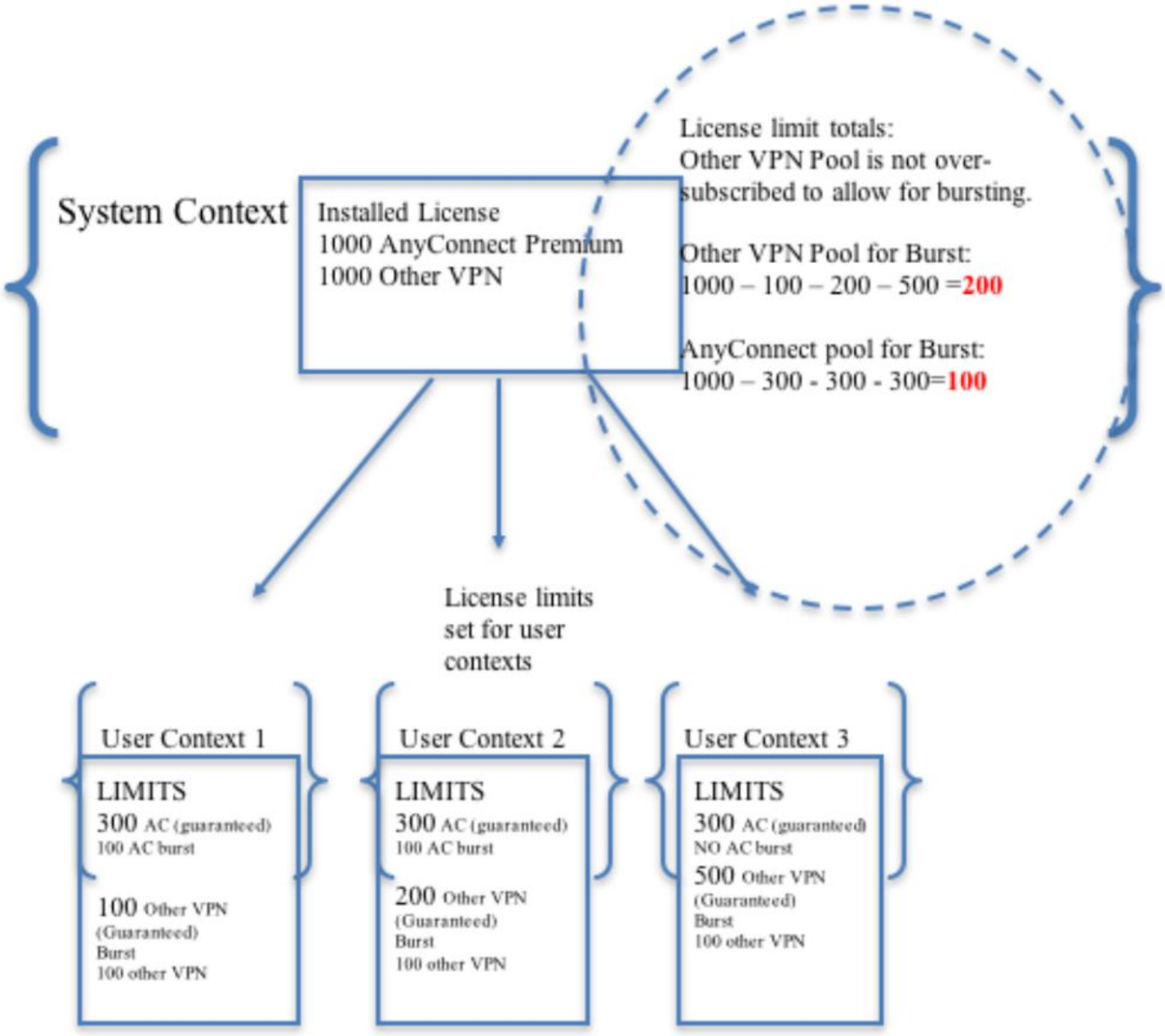
Schritt 2: Zuweisung von VPN-Ressourcen

Konfiguriert über vorhandene Klassenkonfiguration. Lizenzen sind nach Anzahl der Lizenzen bzw. % der Gesamtzahl pro Kontext zulässig.

Einführung neuer Ressourcentypen für MC RAVPN:

- VPN AnyConnect: Garantiert für einen Kontext und nicht überbelegt
- VPN Burst AnyConnect: Erlauben Sie kontextbezogene zusätzliche Lizenzen, die über das garantierte Limit hinausgehen. Burst-Pool besteht aus Lizenzen, die für einen Kontext nicht garantiert sind, und die in einen Bursting-Kontext auf der Basis des "First-come-first-server"-Verfahrens umgewandelt werden können.

VPN-Lizenzbereitstellungsmodell:



Hinweis: Die ASA5585 bietet maximal 10.000 Cisco AnyConnect-Benutzersitzungen. In diesem Beispiel werden pro Kontext 4.000 Cisco AnyConnect-Benutzersitzungen zugewiesen.

```
class resource02
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000

class resource01
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000
```

Schritt 3: Kontexte konfigurieren und Ressourcen zuweisen

Hinweis: In diesem Beispiel wird GigabitEthernet0/0 von allen Kontexten gemeinsam genutzt.

```
admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin

context context1
  member resource01
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

Schritt 4: Überprüfen Sie, ob die Apex-Lizenz auf der ASA installiert ist. Weitere Informationen finden Sie unter dem Link.

Aktivieren oder Deaktivieren von Aktivierungsschlüsseln

Schritt 5: Konfigurieren Sie ein AnyConnect-Image-Paket. Je nach verwendeter ASA-Version gibt es zwei Möglichkeiten, AnyConnect-Image zu laden und für RA VPN zu konfigurieren. Wenn die Version 9.6.2 und höher ist, kann die Flash-Virtualisierung verwendet werden. Für ältere Versionen als 9.6.2 siehe Anhang A

> **Hinweis:** Ab Version 9.6.2 wird Flash-Virtualisierung unterstützt, d. h. wir können ein AnyConnect-Image pro Kontext verwenden.

Flash-Virtualisierung

VPN für den Remote-Zugriff erfordert Flash-Speicher für verschiedene Konfigurationen und Bilder wie AnyConnect-Pakete, Hostscan-Pakete, DAP-Konfiguration, Plugins, Anpassung und Lokalisierung usw. Im Multi-Context-Modus vor 9.6.2 können Benutzerkontexte nicht auf einen beliebigen Teil des Flash-Speichers zugreifen, und der Flash-Speicher wird vom Systemadministrator nur über den Systemkontext verwaltet und zugänglich.

Um diese Einschränkung zu beheben und gleichzeitig die Sicherheit und den Datenschutz von Dateien im Flash-Speicher zu wahren sowie den Flash-Speicher fair unter Kontexten freizugeben, wird ein virtuelles Dateisystem für den Flash im Multi-Context-Modus erstellt. Diese Funktion soll es ermöglichen, AnyConnect-Images auf Kontextbasis zu konfigurieren und nicht global zu konfigurieren. Dadurch können verschiedene Benutzer verschiedene AnyConnect-Images installieren. Darüber hinaus kann durch die Freigabe von AnyConnect-Images die von diesen Images benötigte Speicherkapazität verringert werden. Der gemeinsam genutzte Speicher wird zum Speichern von Dateien und Paketen verwendet, die in allen Kontexten gleich sind.

> **Hinweis:** Der Systemkontexteadministrator hat weiterhin vollständigen Lese- und Schreibzugriff auf den gesamten Flash-Speicher und die privaten und gemeinsam genutzten Speicherdateisysteme.Der Systemadministrator muss eine Verzeichnisstruktur erstellen und alle privaten Dateien und freigegebenen Dateien in verschiedene Verzeichnisse

organisieren, sodass diese Verzeichnisse für Kontexte konfiguriert werden können, die als gemeinsam genutzter Speicher bzw. als privater Speicher zugreifen.

Jeder Kontext verfügt über Lese-/Schreib-/Löschrechte für seinen eigenen privaten Speicher und hat nur Lesezugriff auf seinen freigegebenen Speicher. Nur der Systemkontext hat Schreibzugriff auf den freigegebenen Speicher..

In den folgenden Konfigurationen wird der benutzerdefinierte Kontext 1 zur Darstellung des privaten Speichers konfiguriert, und der benutzerdefinierte Kontext 2 wird zur Darstellung des gemeinsam genutzten Speichers konfiguriert.

Privater Speicher

Sie können einen privaten Speicherplatz pro Kontext angeben. Sie können aus diesem Verzeichnis im Kontext lesen/schreiben/löschen (sowie aus dem Systemausführungsbereich). Unter dem angegebenen Pfad erstellt die ASA ein Unterverzeichnis, das nach dem Kontext benannt ist.

Wenn Sie beispielsweise für context1 disk0:/private-storage für den Pfad angeben, erstellt die ASA ein Unterverzeichnis für diesen Kontext auf disk0:/private-storage/context1/.

Gemeinsam genutzter Speicher

Pro Kontext kann ein schreibgeschützter gemeinsam genutzter Speicherplatz angegeben werden. Um die Duplizierung allgemeiner großer Dateien zu reduzieren, die von allen Kontexten gemeinsam genutzt werden können (z. B. AnyConnect-Pakete), kann gemeinsam genutzter Speicherplatz verwendet werden.

Konfigurationen zur Verwendung des privaten Speicherplatzes

```
!! Create a directory in the system context.
ciscoasa(config)# mkdir private_context1

!! Define the directory as private storage url in the respective context.

ciscoasa(config)# context context1 ciscoasa(config-ctx)# storage-url private
disk0:/private_context1 context1

!! Transfer the anyconnect image in the sub directory.
ciscoasa(config)# copy flash:/anyconnect-win-4.2.01035-k9.pkg flash:/private_context1/context1
```

Konfigurationen für die Nutzung des freigegebenen Speicherplatzes

```
!! Create a directory in the system context.

ciscoasa(config)# mkdir shared

!! Define the directory as shared storage url in the respective contexts.

ciscoasa(config)# context context2 ciscoasa(config-ctx)# storage-url shared disk0:/shared shared

!! Transfer the anyconnect image in the shared directory.
ciscoasa(config)# copy disk0:/anyconnect-win-4.3.05019-k9.pkg disk0:/shared
```

Überprüfen Sie das Bild unter den entsprechenden Kontexten.

```
!! Custom Context 1 configured for private storage.

ciscoasa(config)#changeto context context1
ciscoasa/context1(config)# show context1:
213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

!! Custom Context 2 configured for shared storage.

ciscoasa(config)#changeto context context2
ciscoasa/context2(config)# show shared:
195 25356342 May 24 2017 08:07:02 shared:/anyconnect-win-4.3.05017-k9.pkg
```

Schritt 6: Im Folgenden finden Sie eine Zusammenfassung der Konfigurationen im Systemkontext mit den oben beschriebenen Flash-Virtualisierungskonfigurationen:

Systemkontext

```
context context1
member resource01
allocate-interface GigabitEthernet0/0
 storage-url private disk0:/private_context1 context1
config-url disk0:/context1.cfg
join-failover-group 1
!
context context2
member resource02
allocate-interface GigabitEthernet0/1
storage-url shared disk0:/shared shared
config-url disk0:/context2.cfg
join-failover-group 2
```

Schritt 7: Konfigurieren Sie die beiden benutzerdefinierten Kontexte wie unten gezeigt.

Benutzerdefinierter Kontext 1

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0
username cisco password cisco

!! Configure the required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
```

```
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
```

Benutzerdefinierter Kontext 2

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image shared:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0
username cisco password cisco

!! Configure the required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com
!
!
tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
```

Überprüfen

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

Überprüfen, ob Apex-Lizenz installiert ist

ASA erkennt keine AnyConnect Apex-Lizenz spezifisch an, setzt jedoch die Lizenzmerkmale einer Apex-Lizenz durch, z. B.:

- AnyConnect Premium-Lizenz für Plattformlimit
- AnyConnect für Mobile
- AnyConnect für Cisco VPN-Telefon
- Erweiterte Endgerätebewertung

Ein Syslog wird erstellt, wenn eine Verbindung blockiert wird, weil keine AnyConnect Apex-Lizenz installiert ist.

Überprüfen, ob das AnyConnect-Paket in benutzerdefinierten Kontexten (9.6.2 und höher) verfügbar ist

```
! AnyConnect package is available in context1

 ciscoasa/context1(config)# show context1:

213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

Falls das Bild nicht im benutzerdefinierten Kontext vorhanden ist, verweisen Sie bitte auf die AnyConnect-Image-Konfiguration (9.6.2 und höher).

Überprüfen, ob Benutzer über AnyConnect in benutzerdefinierten Kontexten eine Verbindung herstellen können

Tipp: Für eine bessere Anzeige sehen Sie sich Videos im Vollbildmodus an.

```
!! One Active Connection on Context1

ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 5
Assigned IP : 192.168.1.1 Public IP : 10.142.168.102
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Mobile
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 3186 Bytes Rx : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time : 15:33:25 UTC Thu Dec 3 2015
Duration : 0h:00m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2
```

```
ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2

ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 1
Assigned IP : 192.168.51.1 Public IP : 10.142.168.94
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 10550 Bytes Rx : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
Login Time : 15:34:16 UTC Thu Dec 3 2015
Duration : 0h:00m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none

!! Changing Context to System

ciscoasa/pri/context2/act# changeto system

!! Notice total number of connections are two (for the device)

ciscoasa/pri/act# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
Status : Capacity : Installed : Limit
----------------------------------------
AnyConnect Premium : ENABLED : 10000 : 10000 : NONE
Other VPN (Available by Default) : ENABLED : 10000 : 10000 : NONE
AnyConnect for Mobile : ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment : ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone : ENABLED
VPN-3DES-AES : ENABLED
VPN-DES : ENABLED
----------------------------------------------------------------------------

----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
Local : Shared : All : Peak : Eff. :
In Use : In Use : In Use : In Use : Limit : Usage
-------------------------------------------------
AnyConnect Premium : 2 : 0 : 2 : 2 : 10000 : 0%
AnyConnect Client : : 2 : 2 : 0%
AnyConnect Mobile : : 2 : 2 : 0%
Other VPN : : 0 : 0 : 10000 : 0%
Site-to-Site VPN : : 0 : 0 : 0%
----------------------------------------------------------------------------

!! Notice the resource usage per Context

ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
Resource Current Peak Limit Denied Context
AnyConnect 1 1 4000 0 context1
AnyConnect 1 1 4000 0 context2
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Fehlerbehebung bei AnyConnect

> **Tipp:** Falls auf der ASA keine Apex-Lizenz installiert ist, wird die AnyConnect-Sitzung mit dem folgenden Syslog beendet:
>
> %ASA-6-725002: Gerät hat SSL-Handshake mit Client OUTSIDE:10.142.168.86/51577 bis 10.106.44.38/443 für TLSv1-Sitzung abgeschlossen
> %ASA-6-113012: AAA-Benutzerauthentifizierung erfolgreich: Lokale Datenbank: Benutzer = cisco
> %ASA-6-113009: Über AAA abgerufene Standardgruppenrichtlinie (GroupPolicy_MC_RAVPN_1) für Benutzer = cisco
> %ASA-6-113008: AAA-Transaktionsstatus AKZEPTIEREN: Benutzer = cisco
> %ASA-3-716057: Gruppen-Benutzer-IP <10.142.168.86> Sitzung beendet, keine AnyConnect Apex-Lizenz verfügbar
> %ASA-4-113038: Gruppen-Benutzer-IP <10.142.168.86> Die übergeordnete AnyConnect-Sitzung kann nicht erstellt werden.

Anhang A: Konfiguration von AnyConnect-Images für Versionen vor 9.6.2

Das AnyConnect-Image wird im Admin-Kontext für ASA-Versionen vor 9.6.2 global konfiguriert (beachten Sie, dass die Funktion ab 9.5.2 verfügbar ist), da der Flash-Speicher nicht virtualisiert ist und nur vom Systemkontext aus zugänglich ist.

Schritt 5.1. Kopieren Sie die AnyConnect-Paketdatei im Systemkontext in den Flash-Speicher.

Systemkontext:

```
ciscoasa(config)# show flash:

195 25356342 May 24 2017 08:07:02 anyconnect-win-4.3.05017-k9.pkg
```

Schritt 5.2: Konfigurieren des AnyConnect-Images im Admin-Kontext.

Admin-Kontext:

```
webvpn
anyconnect image disk0:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
```

Hinweis: AnyConnect-Image kann nur im Admin-Kontext konfiguriert werden. Alle Kontexte beziehen sich automatisch auf diese globale AnyConnect-Image-Konfiguration.

Benutzerdefinierter Kontext 1:

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.38 255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
group-url https://10.106.44.38/context1 enable
```

Benutzerdefinierter Kontext 2:

```
!! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.36 255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN
```

```
group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
group-url https://10.106.44.36/context2 enable
```

Überprüfen, ob das AnyConnect-Paket im Admin-Kontext installiert ist und in benutzerdefinierten Kontexten verfügbar ist (vor 9.6.2)

```
!! AnyConnect package is installed in Admin Context

ciscoasa/pri/admin/act# show run webvpn
webvpn
anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
anyconnect enable

ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1

ciscoasa/pri/admin/act# changeto context context1

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable OUTSIDE
anyconnect enable
tunnel-group-list enable

ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed
```

Referenzen

[Versionshinweise: 9,5(2)]

[Versionshinweise: 9,6(2)]

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Leitfaden zur Fehlerbehebung bei AnyConnect VPN-Clients - Häufige Probleme
- Verwalten, Überwachen und Beheben von AnyConnect-Sitzungen
- Technischer Support und Dokumentation - Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf