ASA: VPN ad accesso remoto in modalità multi-contesto (AnyConnect)

Introduzione

In questo documento viene descritto come configurare la VPN (Virtual Private Network) di Accesso remoto su firewall di Cisco Adaptive Security Appliance (ASA) in modalità contesto multiplo (MC) tramite la CLI. Mostra Cisco ASA in più funzionalità supportate/non supportate in modalità contesto e i requisiti delle licenze per la VPN ASA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione ASA AnyConnect SSL
- Configurazione di più contesti ASA

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AnyConnect Secure Mobility Client versione 4.4.0243
- Due ASA5525 con software ASA versione 9.6(2)

Nota: Scaricare il pacchetto AnyConnect VPN Client da Download software Cisco (solo utenti registrati).

Nota: Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il contesto multiplo è una forma di virtualizzazione che consente l'esecuzione simultanea di più copie indipendenti di un'applicazione sullo stesso hardware, con ogni copia (o dispositivo virtuale) visualizzata come un dispositivo fisico separato per l'utente. Ciò permette a più utenti indipendenti di visualizzare una singola appliance ASA come più appliance. Dalla versione iniziale, la famiglia ASA supporta firewall virtuali; tuttavia, l'appliance ASA non supporta la virtualizzazione per l'accesso remoto. Il supporto VPN LAN2LAN (L2L) per il multi-contesto è stato aggiunto per la release 9.0.

Nota: A partire dalla versione **9.5.2,** il supporto della virtualizzazione basata su più contesti per le connessioni di accesso remoto VPN all'appliance ASA.

Dalla versione **9.6.2** abbiamo il supporto per la virtualizzazione Flash, ossia possiamo avere un'immagine Anyconnect per contesto.

Cronologia funzionalità per multicontext

Nuove funzionalità aggiunte in ASA 9.6(2)

Funzionalità	Descrizione
Funzionalità Pre-fill/Username-from-cert per modalità contesto multipla	Il supporto SSL di AnyConnect è esteso e consente di abilitare le CLI con funzionalità pre-compilazione/nome utente da certificato, disponibili in precedenza solo in modalità singola, anche in modalità contesto multiplo.
Virtualizzazione flash per VPN ad accesso remoto	La VPN ad accesso remoto in modalità contesto multiplo ora supporta la virtualizzazione flash. Ogni contesto può avere uno spazio di storage privato e uno spazio di storage condiviso basato sul flash totale disponibile.
Profili client AnyConnect supportati nei dispositivi multi-contesto	I profili client AnyConnect sono supportati nei dispositivi multi-contesto. Per aggiungere un nuovo profilo utilizzando ASDM, è necessario avere AnyConnect Secure Mobility Client versione 4.2.00748 o 4.3.03013 e successive.
Failover stateful per connessioni AnyConnect in modalità contesto multiplo	Il failover stateful è ora supportato per le connessioni AnyConnect in modalità più contesto.
I criteri di accesso dinamico VPN (DAP) di Accesso remoto sono supportati in modalità a più contesti	Èora possibile configurare DAP per contesto in modalità contesto multiplo.
La VPN CoA (Change of Authorization) ad accesso remoto è supportata in modalità contesto multiplo	Èora possibile configurare CoA per contesto in modalità contesto multiplo.
Localizzazione VPN di Accesso remoto supportata in modalità contesto multiplo	La localizzazione è supportata a livello globale. Esiste un solo insieme di file di localizzazione condivisi in contesti diversi.
L'archiviazione di acquisizione pacchetti per contesto è supportata.	Lo scopo di questa funzione è quello di consentire all'utente di copiare un'acquisizione direttamente da un contesto allo storage esterno o al contesto dello storage privato su flash. Questa funzione consente inoltre di copiare l'acquisizione raw negli strumenti di acquisizione dei pacchetti esterni, ad esempio wire-shark, da un contesto.

Funzioni di ASA 9.5(2)

Funzionalità	Descrizione

AnyConnect 4.x e versioni successive (solo VPN SSL; non supporta IKEv2)	Supporto della virtualizzazione basata sul contesto per le connessioni di acce remoto VPN all'appliance ASA.
Configurazione centralizzata dell'immagine AnyConnect	• Lo storage flash non è virtualizzato. • L'immagine AnyConnect è configurata a livello globale nel contesto admi configurazione si applica a tutti i contesti
Aggiornamento immagine AnyConnect	I profili client AnyConnect sono supportati nei dispositivi multi-contesto. Per aggiungere un nuovo profilo utilizzando ASDM, è necessario avere AnyConn Secure Mobility Client versione 4.2.00748 o 4.3.03013 e successive.
Gestione risorse di contesto per le connessioni AnyConnect	• Configurabilità per controllare l'utilizzo massimo della licenza per contest • Configurabilità per consentire la frammentazione della licenza per contes

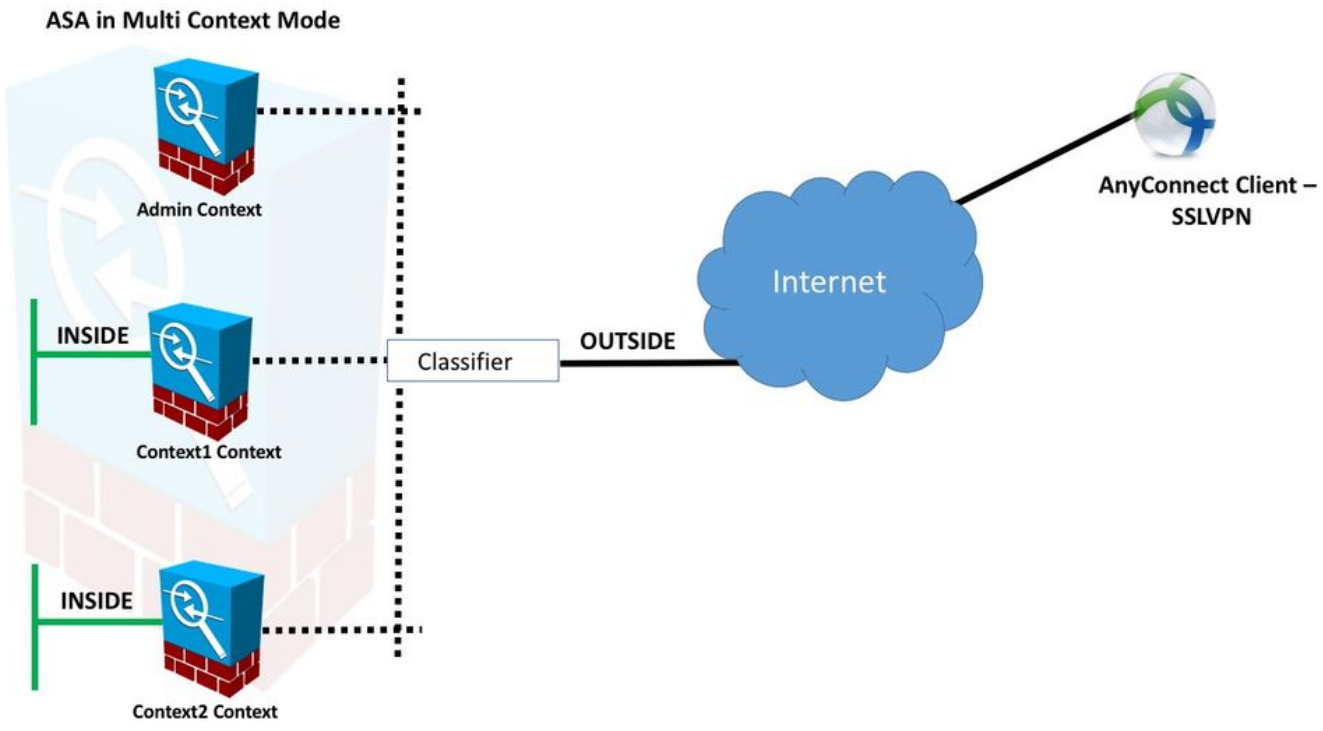
Licenze

- Richiesta licenza AnyConnect Apex
- Licenze Essentials ignorate/non consentite
- Configurabilità per controllare l'utilizzo massimo della licenza per contesto
- Configurabilità per consentire la frammentazione della licenza per contesto

Configurazione

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi (solo utenti registrati).]

Esempio di rete



Nota: Più contesti in questo esempio condividono un'interfaccia (OUTSIDE), quindi il classificatore utilizza l'interfaccia indirizzi MAC univoci (automatici o manuali) per inoltrare i pacchetti. Per ulteriori informazioni sulla classificazione dei pacchetti in più contesti da parte dell'appliance di sicurezza, consultare la sezione Modalità di classificazione dei pacchetti da parte dell'ASA

La seguente procedura di configurazione è basata sulla versione ASA 9.6.2 e successive, che illustra alcune delle nuove funzionalità disponibili. Le differenze nella procedura di configurazione delle versioni ASA precedenti alla 9.6.2 (e successive alla 9.5.2) sono documentate nell'Appendice A del documento.

Di seguito sono descritte le configurazioni necessarie nel contesto di sistema e nei contesti personalizzati per la configurazione della VPN ad accesso remoto:

Configurazioni iniziali nel contesto di sistema

Per iniziare, in Contesto di sistema configurare il failover, l'allocazione delle risorse VPN, i contesti personalizzati e la verifica della licenza Apex. La procedura e le configurazioni sono descritte in questa sezione e nella sezione successiva

Passaggio 1. Configurazione di failover.

```
 !! 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
```

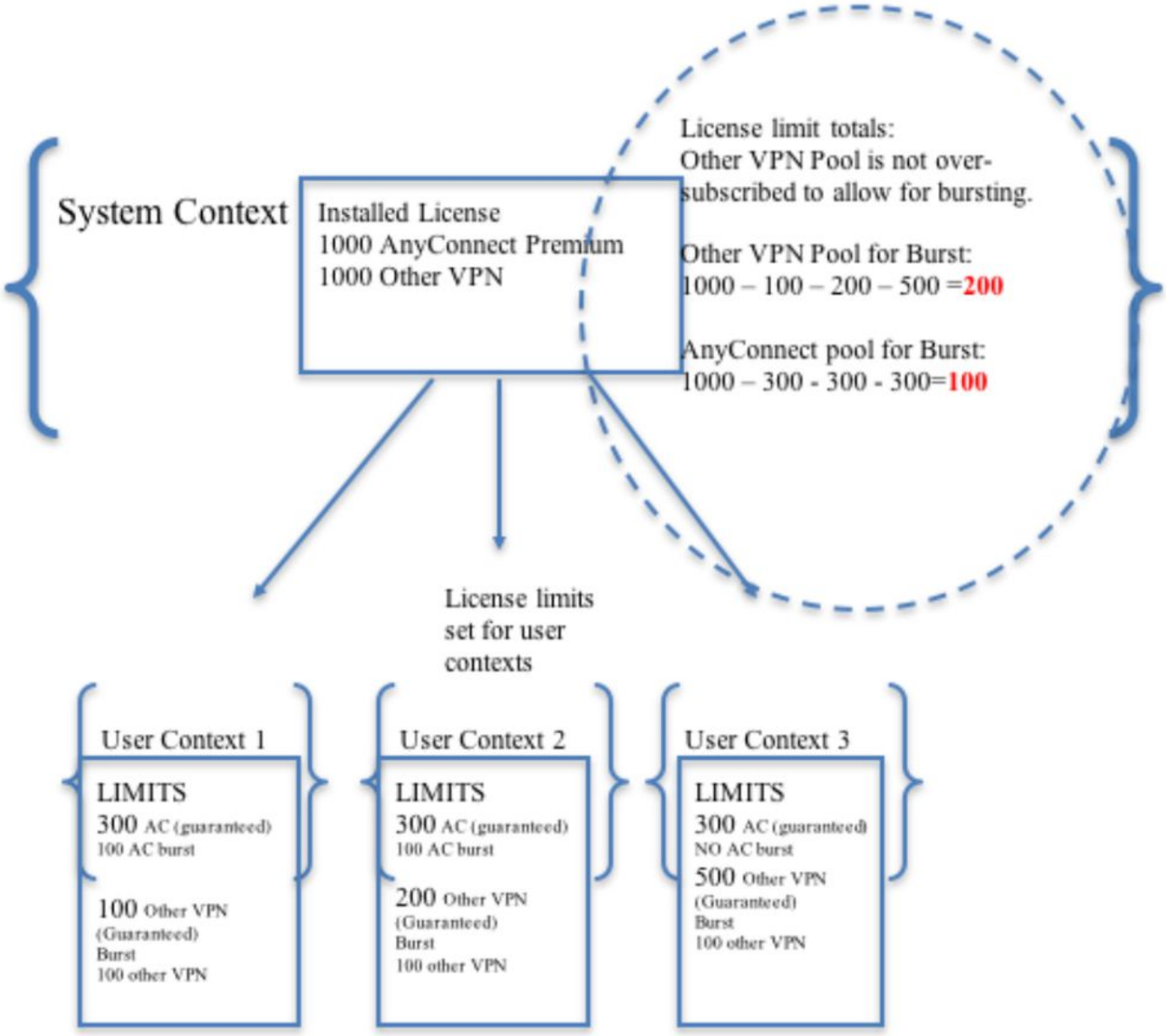
Passaggio 2. Allocare le risorse VPN.

Configurato tramite la configurazione di classe esistente. Le licenze sono consentite in base al numero di licenze o alla percentuale del totale per contesto

Nuovi tipi di risorse introdotti per MC RAVPN:

- VPN AnyConnect: Garantito per un contesto e non può essere sovrascritto
- VPN Burst AnyConnect: Consenti licenze aggiuntive al contesto oltre il limite garantito. Il pool burst è costituito da qualsiasi licenza non garantita per un contesto e può essere frammentato in base al tipo di servizio disponibile per la prima volta

Modello di provisioning licenze VPN:



Nota: ASA5585 offre un massimo di 10.000 sessioni utente Cisco AnyConnect e nell'esempio, vengono allocate 4000 sessioni utente Cisco AnyConnect per contesto.

```
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
```

Passaggio 3. Configurare i contesti e assegnare le risorse.

Nota: nell'esempio, Gigabit Ethernet0/0 è condiviso tra tutti i contesti.

```
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
```

Passaggio 4. Verificare che la licenza Apex sia installata sull'appliance ASA, quindi fare riferimento al collegamento seguente per ulteriori dettagli.

Attivazione o disattivazione delle chiavi di attivazione

Passaggio 5. Configurare un pacchetto immagine Anyconnect. A seconda della versione ASA in uso, sono disponibili due modi per caricare l'immagine Anyconnect e configurare la VPN ASA. Se la versione è 9.6.2 o successiva, è possibile utilizzare la virtualizzazione Flash. Per le versioni precedenti alla 9.6.2, fare riferimento all'Appendice A

> **Nota:** Nella versione 9.6.2 e successive, abbiamo il supporto per la virtualizzazione Flash, il che significa che possiamo avere un'immagine Anyconnect per contesto.

Virtualizzazione Flash

La VPN ad accesso remoto richiede lo storage flash per diverse configurazioni e immagini, come pacchetti AnyConnect, pacchetti hostscan, configurazione DAP, plug-in, personalizzazione e localizzazione, ecc. Nella modalità multi-contesto precedente alla 9.6.2, i contesti utente non possono accedere a nessuna parte della memoria flash e quest'ultima è gestita e accessibile solo dal contesto di sistema.

Per risolvere questo problema, mantenendo la sicurezza e la privacy dei file sulla memoria flash e consentendo una condivisione equa della memoria flash tra i contesti, viene creato un file system virtuale per la memoria flash in modalità multi-contesto. Lo scopo di questa funzione è quello di consentire la configurazione delle immagini AnyConnect per contesto anziché configurarle globalmente. Ciò consente a diversi utenti di avere diverse immagini AnyConnect installate. Inoltre, consentendo la condivisione delle immagini AnyConnect, è possibile ridurre la quantità di memoria utilizzata da queste immagini. La memoria condivisa viene utilizzata per archiviare file e pacchetti comuni a tutti i contesti.

> **Nota:** L'amministratore di contesto del sistema continuerà ad avere accesso completo in lettura/scrittura all'intero flash e ai file system di memorizzazione privata e condivisa. L'amministratore di sistema dovrà creare una struttura di directory e organizzare tutti i file privati e condivisi in directory diverse in modo che queste directory possano essere

configurate per l'accesso ai contesti rispettivamente come memoria condivisa e memorizzazione privata.

Ogni contesto disporrà di autorizzazioni di lettura/scrittura/eliminazione per il proprio archivio privato e avrà accesso in sola lettura al relativo archivio condiviso. Solo il contesto di sistema avrà accesso in scrittura allo storage condiviso.

Nelle configurazioni seguenti, il contesto personalizzato 1 verrà configurato per illustrare l'archiviazione privata e il contesto personalizzato 2 verrà configurato per illustrare l'archiviazione condivisa.

Ammasso privato

È possibile specificare uno spazio di archiviazione privato per contesto. È possibile leggere/scrivere/eliminare da questa directory all'interno del contesto (nonché dallo spazio di esecuzione del sistema). Sotto il percorso specificato, l'ASA crea una sottodirectory con il nome del contesto.

Ad esempio, per context1 se si specifica disk0:/private-storage per il percorso, l'ASA crea una sottodirectory per questo contesto in disk0:/private-storage/context1/.

Storage condiviso

È possibile specificare uno spazio di archiviazione condiviso di sola lettura per contesto. Per ridurre la duplicazione dei file di grandi dimensioni comuni che possono essere condivisi tra tutti i contesti (ad esempio i pacchetti AnyConnect), è possibile usare uno spazio di archiviazione condiviso.

Configurazioni per l'utilizzo dello spazio di archiviazione privato

```
!! 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
```

Configurazioni per l'utilizzo dello spazio di archiviazione condiviso

```
!! 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
```

Verificare l'immagine nei rispettivi contesti

```
!! 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
```

Passaggio 6. Di seguito è riportato il riepilogo delle configurazioni nel contesto del sistema che include le configurazioni di virtualizzazione flash descritte sopra:

Contesto di sistema

```
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
```

Passaggio 7: Configurare i due contesti personalizzati come illustrato di seguito

Contesto personalizzato 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
```

Contesto personalizzato 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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Verifica dell'installazione della licenza Apex

L'ASA non riconosce specificamente una licenza AnyConnect Apex, ma applica le caratteristiche della licenza di una licenza Apex, che includono:

- AnyConnect Premium concesso in licenza per il limite della piattaforma
- AnyConnect per Mobile
- AnyConnect per Cisco VPN Phone
- Valutazione avanzata degli endpoint

Quando la connessione è bloccata, viene generato un syslog perché non è installata una licenza AnyConnect Apex.

Verifica della disponibilità del pacchetto AnyConnect in contesti personalizzati (9.6.2 e versioni successive)

```
! 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
```

Se l'immagine non è presente nel contesto personalizzato, consultare la configurazione dell'immagine Anyconnect (9.6.2 e successive).

Verifica della possibilità di connessione degli utenti tramite AnyConnect in contesti personalizzati

Suggerimento: per una visualizzazione migliore guarda i video sotto a schermo intero.

```
!! 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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Risoluzione dei problemi di AnyConnect

> **Suggerimento:** Se l'appliance ASA non ha una licenza Apex installata, la sessione AnyConnect verrà terminata con il seguente syslog:
>
> %ASA-6-72502: Handshake SSL completato con client OUTSIDE:10.142.168.86/51577 a 10.106.44.38/443 per sessione TLSv1
> %ASA-6-113012: Autenticazione utente AAA riuscita: database locale: user = cisco
> %ASA-6-113009: AAA ha recuperato i criteri di gruppo predefiniti (GroupPolicy_MC_RAVPN_1) per l'utente = cisco
> %ASA-6-113008: Stato transazione AAA ACCETTO: user = cisco
> %ASA-3-716057: Gruppo: IP utente <10.142.168.86> Sessione terminata, licenza AnyConnect Apex non disponibile
> %ASA-4-113038: L'IP dell'utente del gruppo <10.142.168.86> non è in grado di creare la sessione padre AnyConnect.

Appendice A - Configurazione dell'immagine Anyconnect per versioni precedenti alla 9.6.2

L'immagine AnyConnect è configurata globalmente nel contesto admin per le versioni ASA precedenti alla 9.6.2 (si noti che la funzionalità è disponibile dalla 9.5.2) perché lo storage flash non è virtualizzato e può essere consultato solo dal contesto del sistema.

Passaggio 5.1. Copiare il file del pacchetto AnyConnect nella memoria flash nel contesto del sistema.

Contesto di sistema:

```
ciscoasa(config)# show flash:

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

Passaggio 5.2. Configurare l'immagine Anyconnect nel contesto Admin.

Contesto amministratore:

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

Nota: L'immagine Anyconnect può essere configurata solo nel contesto di amministrazione. Tutti i contesti fanno automaticamente riferimento a questa configurazione globale dell'immagine Anyconnect.

Contesto personalizzato 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
```

Contesto personalizzato 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
```

Verificare se il pacchetto AnyConnect è installato nel contesto di amministrazione e disponibile nei contesti personalizzati (prima della versione 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
```

Riferimenti

[Note release: 9.5(2)]

[Note release: 9.6(2)]

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Guida alla risoluzione dei problemi dei client VPN AnyConnect - Problemi comuni
- Gestione, monitoraggio e risoluzione dei problemi delle sessioni AnyConnect
- Documentazione e supporto tecnico – Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf