Table of Contents

Preface

Introduction

This cloud connector, known as the Cisco AnyConnect Cloud Web Security Module, gives the AnyConnect client the ability to let Internet web traffic go out through a CWS proxy directly to the destination without forcing it through the organization's headend. Without Cisco CWS, the traffic must be routed down the VPN tunnel,

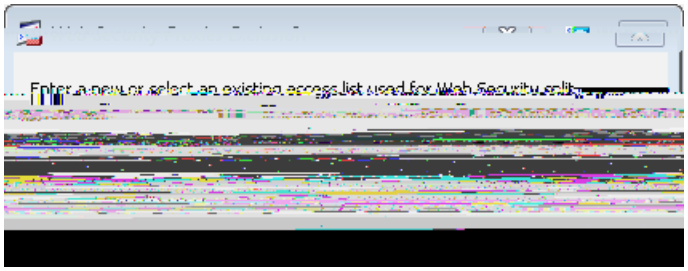
Step 3: Click Add Custom Group.

Step 4:

Step 11:

Step 11: In

Step 5: On the Web Security Proxies Exclusion dialog box, in the Access list name box, enter CWS_Tower_Exclude, and then click Create Access List.



Step 6: On the Access List Result dialog box, review the list of proxies added to the access list, and then click

Step 2:

Step 5: Navigate to the secondary RAVPN Cisco ASA's inside IP address, and then launch Cisco ASDM.

Appendix A: Product List

```
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3.16
 vlan 16
 nameif outside-16
 security-level 0
 ip address 172.16.130.122 255.255.255.0
!
interface GigabitEthernet0/3.17
 vlan 17
 nameif outside-17
 security-level 0
 ip address 172.17.130.122 255.255.255.0
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
```

```
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 10.4.48.0 255.255.255.0 inside
snmp-server host inside 10.4.48.35 community cisco
no snmp-server location
no snmp-server contact
snmp-server community cisco
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
sla monitor 16
 type echo protocol ipIcmpEcho 172.18.1.1 interface outside-16
sla monitor schedule 16 life forever start-time now
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-
SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5
ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set reverse-route
crypto map outside-16_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside-16_map interface outside-16
crypto ca trustpoint VPN-ASA5525X-Trustpoint
 enrollment self
 subject-name CN=VPN-ASA5525X.cisco.local
 keypair VPN-ASA5525X-Keypair
 proxy-ldc-issuer
 crl configure
crypto ca trustpoint VPN-ASA5525X-FO-Trustpoint
 enrollment self
 subject-name CN=VPN-ASA5525X-FO.cisco.local
 keypair VPN-ASA5525X-Keypair
 proxy-ldc-issuer
 crl configure
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=VPN-ASA5525X
```

```
always-on-vpn profile-setting
```

Please use the