ASA 버전 9.2 VPN SGT 분류 및 시행 컨피그레이션 예

목차

소개

이 문서에서는 VPN 사용자를 위해 ASA(Adaptive Security Appliance) 릴리스 9.2.1, TrustSec SGT(Security Group Tag) 분류의 새로운 기능을 사용하는 방법에 대해 설명합니다. 이 예에서는 서로 다른 SGT 및 SGFW(Security Group Firewall)가 할당된 VPN 사용자 2명을 보여 줍니다. SGFW는 VPN 사용자 간의 트래픽을 필터링합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA CLI 컨피그레이션 및 SSL(Secure Socket Layer) VPN 컨피그레이션에 대한 기본 지식
- ASA의 원격 액세스 VPN 구성에 대한 기본 지식
- ISE(Identity Services Engine) 및 TrustSec 서비스에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

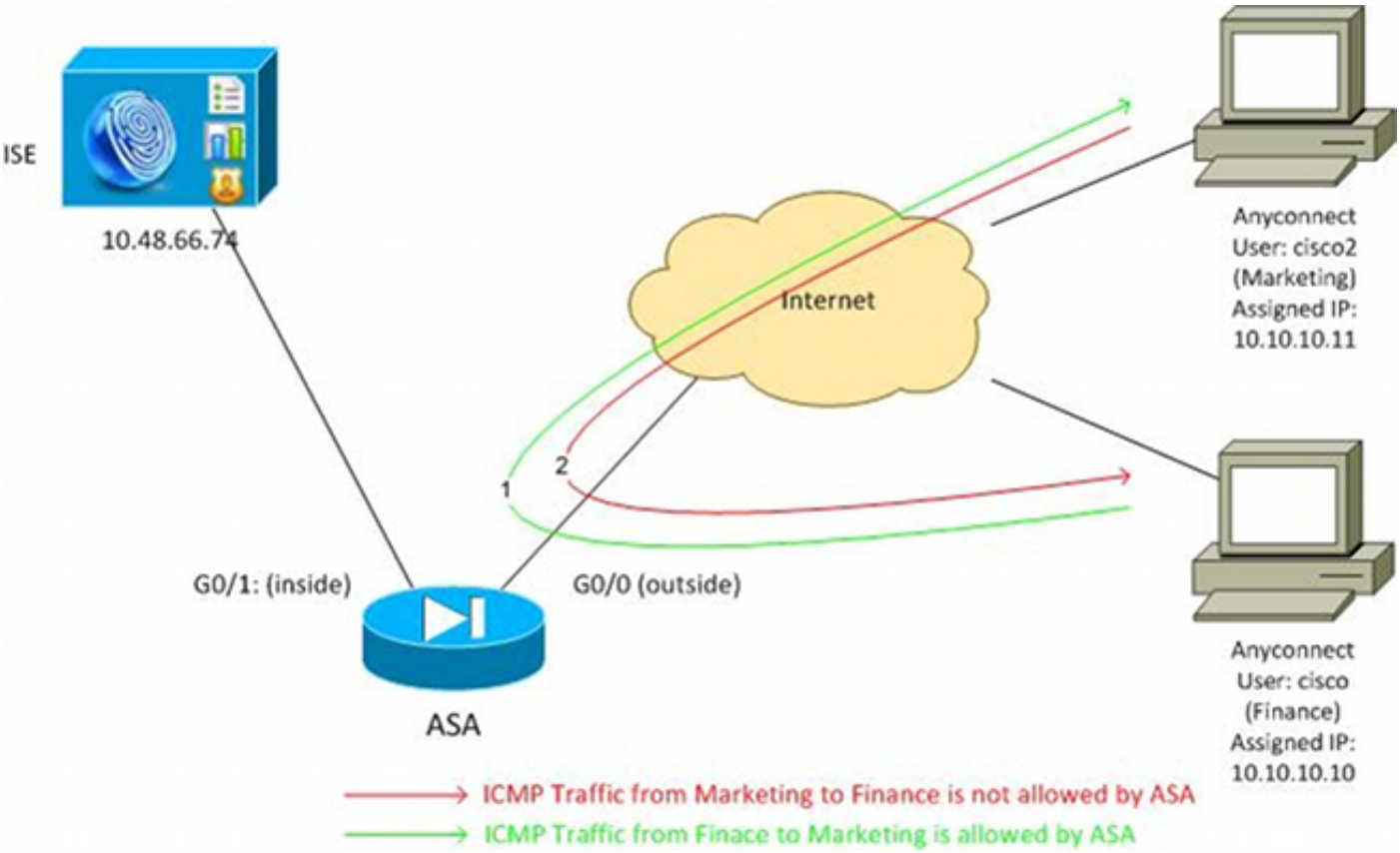
- Cisco ASA 소프트웨어, 버전 9.2 이상
- Cisco AnyConnect Secure Mobility Client가 포함된 Windows 7, 릴리스 3.1
- Cisco ISE, 릴리스 1.2 이상

구성

> **참고**: 이 섹션에서 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용하십시오.

네트워크 다이어그램

VPN 사용자 'cisco'가 재무 팀에 할당되어 마케팅 팀에 대한 ICMP(Internet Control Message Protocol) 연결을 시작할 수 있습니다. VPN 사용자 'cisco2'는 마케팅 팀에 할당되며, 이 경우 연결을 시작할 수 없습니다.

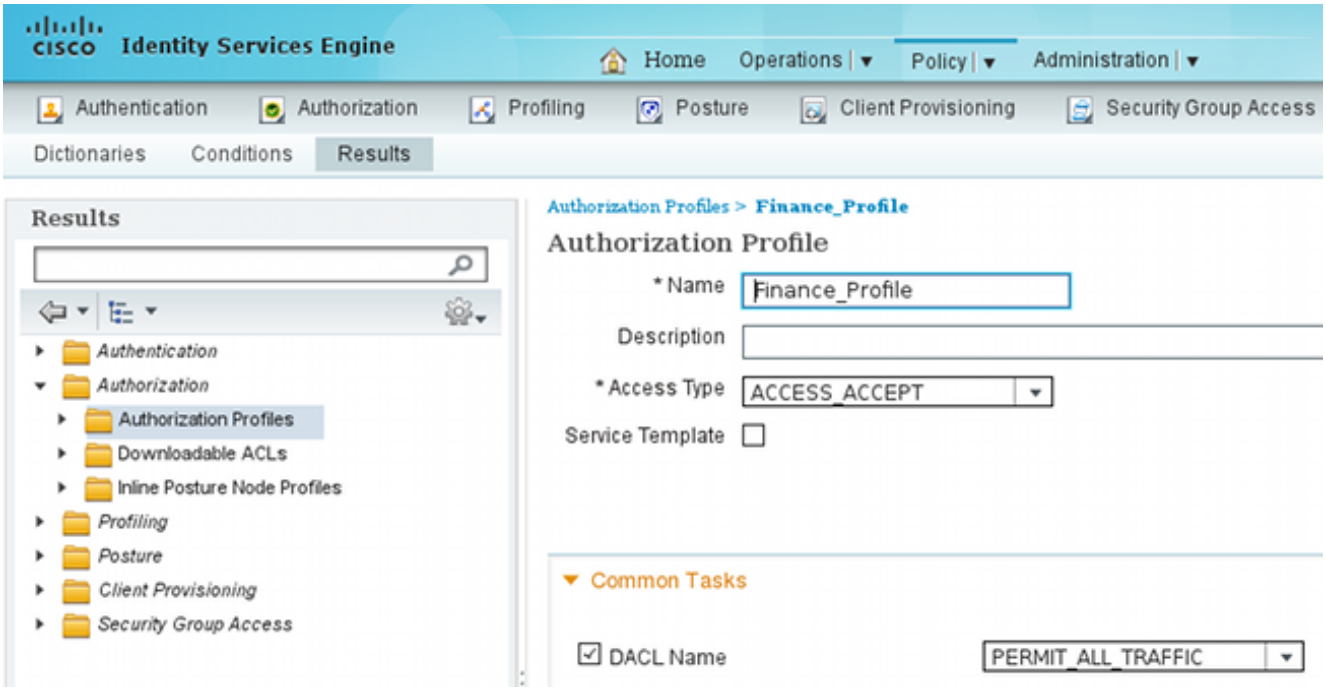


ISE 구성

1. Administration(관리) > **Identity Management(ID 관리) > Identities(ID)**를 선택하여 'cisco'(Finance(재무) 및 'cisco2'(Marketing(마케팅)) 사용자를 추가하고 구성합니다.
2. ASA**를 네트워크 디바이스로** 추가하고 구성하려면 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)를 선택합니다.
3. 재무 및 마케팅 **권한 부여 프로파일을** 추가하고 구성하려면 **Policy > Results > Authorization > Authorization** Profiles를 선택합니다.두 프로파일 모두 모든 트래픽을 허용하는 DACL(Downloadable Access Control List)이라는 하나의 특성만 포함합니다. Finance의 예는

다음과 같습니다

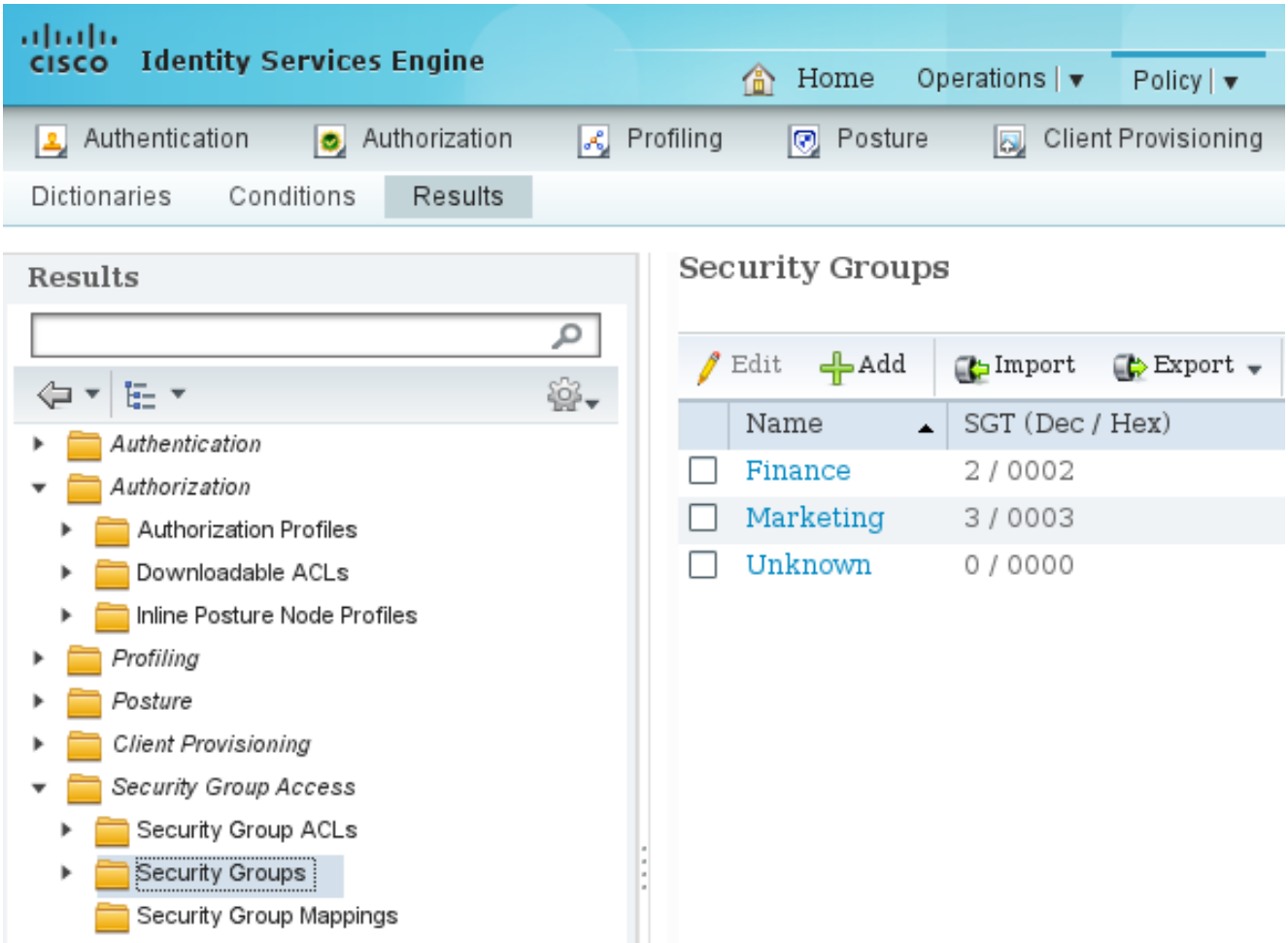
.



각 프로필에는 특정 제한 DACL이 있을 수 있지만 이 시나리오에서는 모든 트래픽이 허용됩니다. 각 VPN 세션에 할당된 DACL이 아니라 SGFW에서 시행을 수행합니다. SGFW로 필터링되는 트래픽은 DACL에서 사용하는 IP 주소 대신 SGT만 사용할 수 있습니다.

4. Finance and Marketing **SGT 그룹을 추가** 하고 **구성하려면 Policy > Results > Security Group Access** > Security Groups를 선택합니다

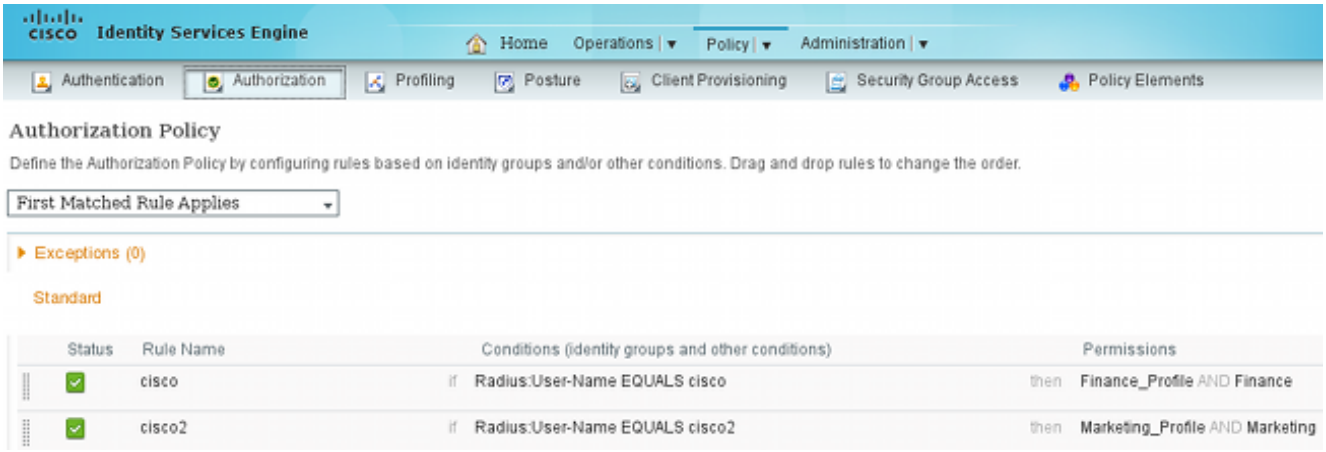
.



5. 두 가지 **권한 부여** 규칙을 구성하려면 Policy(정책) > Authorization(권한 부여)을 선택합니다.

첫 번째 규칙은 SGT 그룹 Finance와 함께 Finance_profile(전체 트래픽을 허용하는 DACL)을 'cisco' 사용자에게 할당합니다. 두 번째 규칙은 SGT 그룹 마케팅과 함께 Marketing_profile(전체 트래픽을 허용하는 DACL)을 'cisco2' 사용자에게 할당합니다

.



ASA 컨피그레이션

1. 기본 VPN 컨피그레이션을 완료합니다.

```
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
```

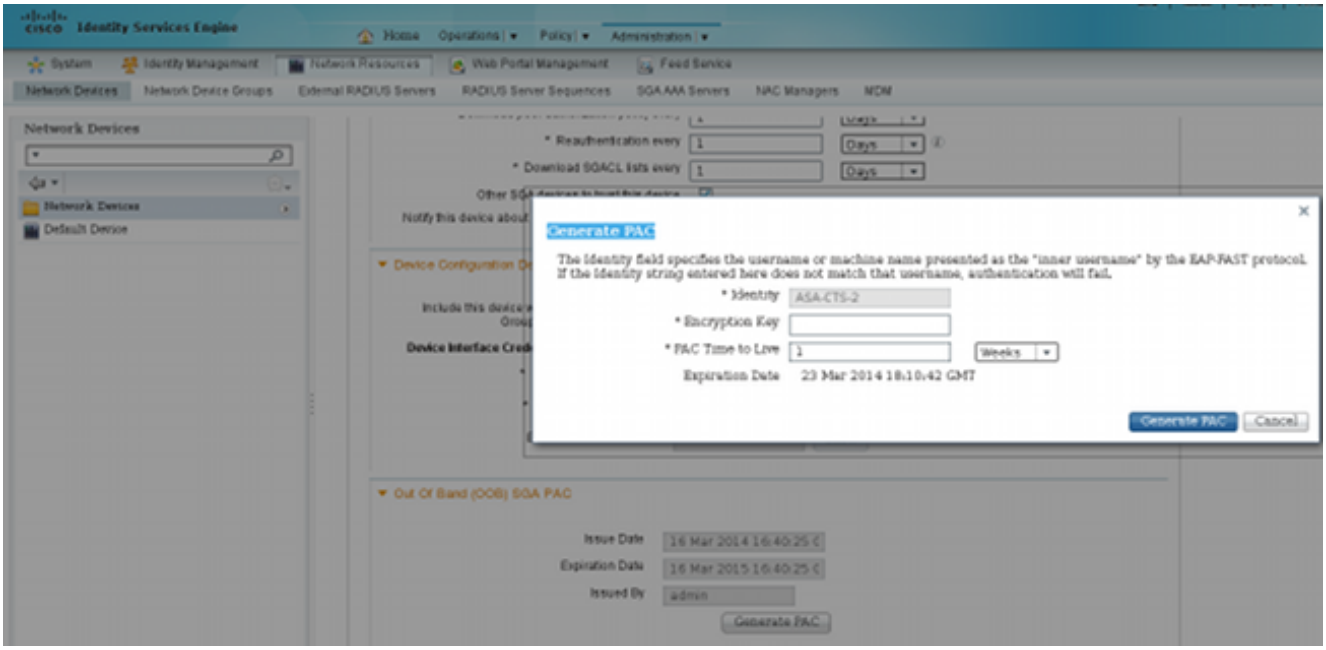
2. ASA AAA 및 TrustSec 컨피그레이션을 완료합니다.

```
aaa-server ISE protocol radius
aaa-server ISE (outside) host 10.48.66.74
 key *****
cts server-group ISE
```

TrustSec 클라우드에 가입하려면 ASA가 PAC(Protected Access Credential)로 인증해야 합니다. ASA는 자동 PAC 프로비저닝을 지원하지 않으므로 ISE에서 파일을 수동으로 생성하고 ASA로 가져와야 합니다.

3. ISE에서 PAC를 생성하려면 **Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > ASA > Advanced TrustSec Settings(고급** TrustSec 설정)를 선택합니다. 파일**을 생성하려면 OOB(Out of Band) PAC** 프로비저닝을 선택합니다

.



4. ASA에 PAC를 가져옵니다.생성된 파일을 HTTP/FTP 서버에 둘 수 있습니다. ASA는 이 옵션을 사용하여 파일을 가져옵니다.

```
ASA# cts import-pac http://192.168.111.1/ASA-CTS-2.pac password 12345678
!PAC Imported Successfully
ASA#
ASA# show cts pac

 PAC-Info:
   Valid until: Mar 16 2015 17:40:25
   AID:         ea48096688d96ef7b94c679a17bdad6f
   I-ID:        ASA-CTS-2
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301
   0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
   e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
   2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
   99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
   11d8378829cc007b91ced9117a
```

올바른 PAC가 있는 경우 ASA는 자동으로 환경 새로고침을 수행합니다. 이렇게 하면 현재 SGT 그룹에 대한 정보가 ISE에서 다운로드됩니다.

```
ASA# show cts environment-data sg-table

Security Group Table:
Valid until: 17:48:12 CET Mar 17 2014
Showing 4 of 4 entries

SG Name                         SG Tag     Type
-------                         ------     -------------
ANY                              65535     unicast
Unknown                              0     unicast
Finance                              2     unicast
Marketing                            3     unicast
```

5. SGFW를 구성합니다. 마지막 단계는 Finance에서 Marketing으로의 ICMP 트래픽을 허용하는 외부 인터페이스에서 ACL을 구성하는 것입니다.

```
access-list outside extended permit icmp security-group tag 2 any security-group
tag 3 any
access-group outside in interface outside
```

또한 태그 대신 보안 그룹 이름을 사용할 수 있습니다.

```
access-list outside extended permit icmp security-group name Finance any
```

security-group name Marketing any

인터페이스 ACL이 VPN 트래픽을 처리하도록 하려면 인터페이스 ACL을 통한 검증 없이 기본적으로 VPN 트래픽을 허용하는 옵션을 비활성화해야 합니다.

no sysopt connection permit-vpn

이제 ASA는 VPN 사용자를 분류하고 SGT를 기반으로 시행을 수행할 준비가 되어 있어야 합니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

이 출력 인터프리터 도구 (등록됨 고객 전용)은 **쇼** 명령을 사용합니다. 분석을 보려면 출력 인터프리터 툴을 사용합니다. **쇼** 명령 출력입니다.

VPN이 설정되면 ASA는 각 세션에 적용된 SGT를 표시합니다.

```
ASA(config)# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 1
Assigned IP  : 10.10.10.10            Public IP    : 192.168.10.68
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 35934                  Bytes Rx     : 79714
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:49:15 CET Sun Mar 16 2014
Duration     : 0h:22m:57s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8700a000010005325d60b
Security Grp : 2:Finance

Username     : cisco2                 Index        : 2
Assigned IP  : 10.10.10.11            Public IP    : 192.168.10.80
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 86171                  Bytes Rx     : 122480
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:52:27 CET Sun Mar 16 2014
Duration     : 0h:19m:45s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8700a000020005325d6cb
Security Grp : 3:Marketing
```

SGFW는 재무(SGT=2)에서 마케팅(SGT=3)으로의 ICMP 트래픽을 허용합니다. 따라서 'cisco' 사용자는 'cisco2' 사용자에게 ping을 수행할 수 있습니다.

```
C:\Users\admin>ping 10.10.10.11 -S 10.10.10.10

Pinging 10.10.10.11 from 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=3ms TTL=128
Reply from 10.10.10.11: bytes=32 time=4ms TTL=128
Reply from 10.10.10.11: bytes=32 time=6ms TTL=128
Reply from 10.10.10.11: bytes=32 time=5ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

카운터가 증가합니다.

```
ASA(config)# show access-list outside
access-list outside; 1 elements; name hash: 0x1a47dec4
access-list outside line 1 extended permit icmp security-group
tag 2(name="Finance") any security-group tag 3(name="Marketing")
any (hitcnt=4) 0x071f07fc
```

연결이 생성되었습니다.

```
Mar 16 2014 18:24:26: %ASA-6-302020: Built inbound ICMP connection for
faddr 10.10.10.10/1(LOCAL\cisco, 2:Finance) gaddr 10.10.10.11/0
laddr 10.10.10.11/0(LOCAL\cisco2, 3:Marketing) (cisco)
```

ICMP 검사가 활성화되었으므로 반환 트래픽이 자동으로 수락됩니다.

Marketing(SGT=3)에서 Finance(SGT=2)로 ping을 시도할 때:

```
C:\Users\admin>ping 10.10.10.10 -S 10.10.10.11

Pinging 10.10.10.10 from 10.10.10.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ASA 보고서:

```
Mar 16 2014 18:06:36: %ASA-4-106023: Deny icmp src outside:10.10.10.11(LOCAL\cisco2,
3:Marketing) dst outside:10.10.10.10(LOCAL\cisco, 2:Finance) (type 8, code 0) by
access-group "outside" [0x0, 0x0]
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

다음 문서를 참조하십시오.

- Catalyst 3750X Series 스위치의 802.1x MACsec을 사용하는 TrustSec 클라우드 구성 예

- ASA 및 Catalyst 3750X Series Switch TrustSec 구성 예 및 문제 해결 가이드

요약

이 문서에서는 VPN 사용자를 분류하고 기본적인 적용을 수행하는 방법에 대한 간단한 예를 제공합니다. SGFW는 또한 VPN 사용자와 네트워크의 나머지 부분 사이의 트래픽을 필터링합니다. SXP(TrustSec SGT Exchange Protocol)를 ASA에서 사용하여 IP와 SGT 간의 매핑 정보를 얻을 수 있습니다. 그러면 ASA가 적절히 분류된 모든 유형의 세션(VPN 또는 LAN)에 대해 시행을 수행할 수 있습니다.

ASA 소프트웨어 버전 9.2 이상에서는 ASA가 RADIUS CoA(Change of Authorization)도 지원합니다(RFC 5176). 성공적인 VPN 상태 후 ISE에서 전송된 RADIUS CoA 패킷에는 규정 준수 사용자를 다른(더 안전한) 그룹에 할당하는 SGT가 포함된 cisco-av-pair가 포함될 수 있습니다. 자세한 예는 관련 정보 섹션의 문서를 참조하십시오.

관련 정보

- ISE를 사용하는 ASA 버전 9.2.1 VPN 상태 컨피그레이션 예
- ASA 및 Catalyst 3750X Series Switch TrustSec 구성 예 및 문제 해결 가이드
- Cisco TrustSec 스위치 컨피그레이션 가이드: Cisco TrustSec 이해
- 보안 어플라이언스 사용자 권한 부여를 위한 외부 서버 구성
- Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.1
- Cisco Identity Services Engine 사용 설명서, 릴리스 1.2
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.