

# 연습 1: DNA Center Segmentation Use Case (데모 시작)

마지막 업데이트: 2018 년 6 월 10 일


**참고:** 인스턴트 데모 시스템을 사용하기 전에 이 가이드를 확인 하십시오. 가이드에서 벗어나지 마십시오. 그렇지 않으면 문제가 발생할 수 있습니다. 본 가이드에 포함되지 않은 시나리오 및 기능은 지원되지 않습니다. 문제가 발생하면 브라우저 캐시를 삭제하고 로그오프한 다음 다시 로그인하십시오.


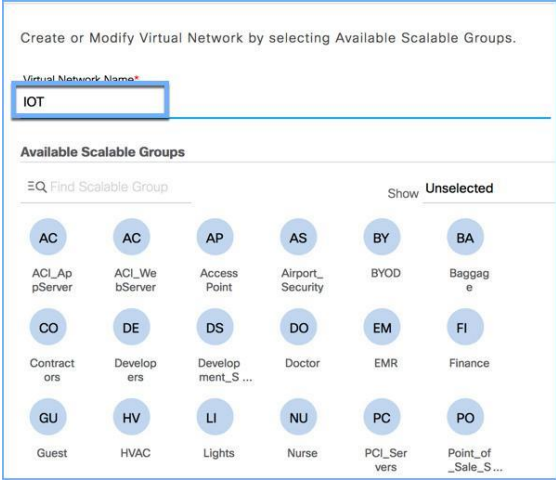
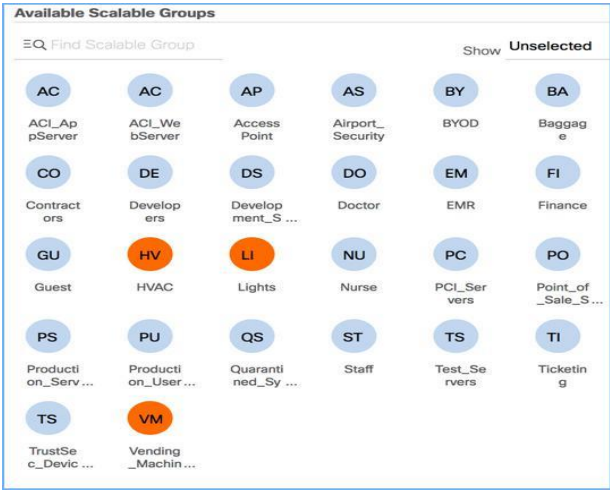
**참고:** Google Chrome 의 incognito mode(시크릿 모드) 로 DNA 센터를 사용해야 합니다.


본 가이드 및 데모에서는 고객이 DNA 센터를 활용하여 현재와 미래의 네트워크 요구 사항을 충족하는 완벽한 보안 정책을 구축하는 방법에 대한 간편함을 보여줍니다. SD-액세스 세그먼테이션에서는 네트워크 수준에서 **가상 네트워크(virtual networks)**를 사용하여 세그먼트할 수 있는 기능이 있고 또한 **확장 가능한 그룹(scalable groups)**을 사용하여 마이크로 세그먼테이션 수준에서 분할할 수 있습니다.

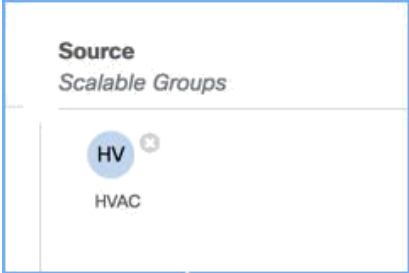
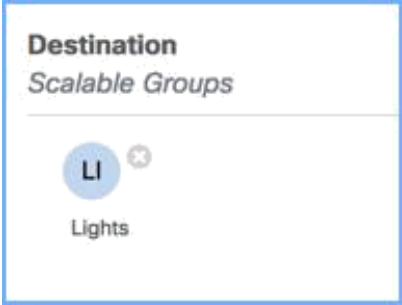
본 데모에서는 다음과 같은 간편함을 전달합니다:


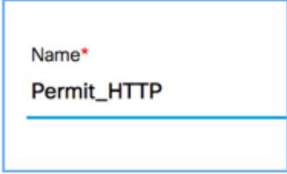
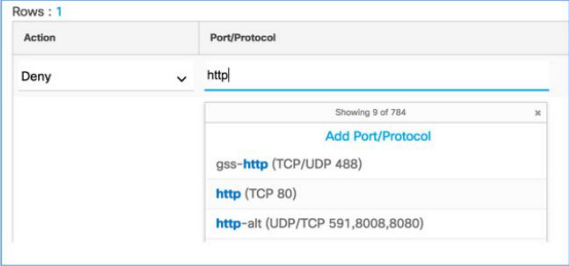
- a. DNA 센터 정책 툴을 사용하여 가상 네트워크 구축
- b. 가상 네트워크에 그룹을 할당.
- c. 보안 정책을 정의하고 구현.
- d. 새로운 보안 구성을 정의.

DIALOG	DEMONSTRATION STEPS
<p>DNA 센터는 캠퍼스 네트워크 내에서 장치를 중앙 집중식으로 구축하고 정책을 관리하기 위한 시스템입니다. DNA 센터는 조직의 보안 관리 구역을 확장하는 동시에 보안 운영 비용을 줄입니다.</p>	<ol style="list-style-type: none"> <li>1. dCloud 에서, <b>View</b> 를 클릭합니다.</li> <li>2. Log in as <b>amdemo1 / C1sco12345</b> 을 사용하여 로그인합니다.</li> <li>3. DNA-C 메인 웹 페이지에서 <b>Policy</b> 를 클릭합니다.</li> </ol> <div data-bbox="902 1562 1357 1696" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  </div>

DIALOG	DEMONSTRATION STEPS
<p>이 단계에서는 가상 네트워크를 구축하기 위해 가상 네트워크 구성합니다. 가상 네트워크를 사용하면 네트워크를 네트워크 레벨러 세그먼트할 수 있습니다. 기존에 사용하던 VRF 와 같은 가상 네트워크를 생각 하면 됩니다.</p>	<p>4. <b>Virtual Network</b> 로 이동합니다:</p> <ol style="list-style-type: none"> <li>새 가상 네트워크 생성합니다.</li> <li>검색 박스 오른쪽에 있는  아이콘을 클릭합니다</li> <li>가상 네트워크(Virtual network)에 이름을 할당합니다.</li> </ol> 
<p>이제 가상 네트워크에 보안 그룹을 할당하겠습니다. 보안 그룹은 디바이스 유형, 사용자 및 디바이스 위치를 기준으로 ISE 에 의해 할당됩니다.</p>	<p>5. 가상 네트워크(Virtual Network)에 그룹을 할당합니다.</p> <ol style="list-style-type: none"> <li>HVAC, Lights 및 Vending Machines 를 선택합니다.</li> </ol>  <p>6. 가상 네트워크의 그룹으로 끌어 놓습니다.</p> <p>7. <b>Save</b> 를 클릭합니다.</p>

DIALOG	DEMONSTRATION STEPS
<p>이제 가상 네트워크를 정의했으므로 이 네트워크에 몇 가지 마이크로 세그먼테이션을 적용할 수 있습니다. 이번 예의 경우에는 HVAC 그룹이 라이트 그룹 (lights group)과 통신하는 것을 원하지 않습니다.</p>	<p>8. <b>Policy Administration</b> 으로 이동합니다:</p> <ol style="list-style-type: none"> <li><b>Group-Based Access Control (Fabric)</b>으로 이동합니다</li> <li>화면 오른쪽의 정책 추가  아이콘을 클릭합니다.</li> </ol> <p>9. 정책 이름을 DENY-HVAC-LIGHTS 로 지정합니다.</p> <div data-bbox="781 596 1164 737" style="border: 1px solid blue; padding: 5px;"> <p>Policy Name*</p> <p><b>DENY-HVAC-LIGHTS</b></p> </div> <p>10. 이제 콘트랙트(Contract)를 할당하겠습니다.</p> <p>11. <b>Add Contract</b> 를 클릭합니다.</p> <ol style="list-style-type: none"> <li>정의된 콘트랙트 목록이 표시됩니다. <b>Deny(거부)</b>를 선택합니다.</li> </ol> <div data-bbox="794 984 1252 1192" style="border: 1px solid blue; padding: 5px;"> <p>≡ Find Contracts</p> <hr/> <p><input type="radio"/> Deny_TFTP_only</p> <p><input checked="" type="radio"/> deny</p> <p><input type="radio"/> permit</p> </div> <ol style="list-style-type: none"> <li><b>Ok</b> 를 클릭합니다.</li> </ol>

DIALOG	DEMONSTRATION STEPS
<p>이제 보안 그룹을 이 정책에 할당하겠습니다. 정책을 생성하면 정책을 한 방향으로 또는 양방향에서 적용할 수 있습니다.</p>	<p>12. <b>Available Scalable Groups</b> 에서 다음과 같이 선택합니다 :</p> <p>a. <b>HVAC</b> 그룹을 선택하고 소스 필드로 이동합니다.</p>  <p>b. <b>Lights</b> 그룹을 선택하고 대상 필드(destination field)로 이동합니다.</p>  <p>13. <b>Save</b> 를 클릭합니다.</p>

DIALOG	DEMONSTRATION STEPS
<p>이제 새 콘트랙트 내에서 제어할 트래픽 유형을 정의합니다.</p>	<p>14. <b>Contracts</b> 로 이동합니다:</p> <ol style="list-style-type: none"> <li>이제 새로운 <b>Access Contract</b> 를 생성하겠습니다.</li> <li><b>Add Contract</b> 를 클릭합니다.</li> </ol>  <p>15. 새 콘트랙트에 <b>Name(이름)</b> 및 <b>Implicit Action</b> 을 지정합니다.</p>  <p>16. <b>Permit</b> 를 <b>Implicit Action</b> 으로 선택합니다.</p> <p>17. 액세스 규칙을 정의합니다.</p> <ol style="list-style-type: none"> <li><b>Deny</b> 를 선택합니다.</li> <li><b>포트/프로토콜에 http</b> 를 입력합니다.</li> </ol>  <ol style="list-style-type: none"> <li>보시다시피 포트와 프로토콜이 이미 적용되었습니다. <b>http(TCP 80)</b>을 선택합니다.</li> <li><b>Save</b> 를 클릭합니다.</li> </ol> <p>18. 이제 새 콘트랙트를 정의했으므로 기존 및 새 정책에 해당 새 콘트랙트를 할당할 수 있습니다.</p>



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)