ASA/PIX: 투명 모드에서 액티브/스탠바이 장애 조치 구성

목차

소개

장애 조치 컨피그레이션에는 전용 장애 조치 링크 및 선택적으로 상태 기반 장애 조치 링크를 통해 서로 연결된 두 개의 동일한 보안 어플라이언스가 필요합니다. 특정 장애 조치 조건이 충족되는지 확인하기 위해 활성 인터페이스 및 유닛의 상태가 모니터링됩니다. 이러한 조건이 충족되면 장애 조치가 발생합니다.

보안 어플라이언스는 두 가지 장애 조치 컨피그레이션을 지원합니다.

- 액티브/액티브 장애 조치
- 액티브/스탠바이 장애 조치

각 장애 조치 컨피그레이션에는 장애 조치를 확인하고 수행하는 고유한 방법이 있습니다. 액티브/액티브 장애 조치를 사용하면 두 유닛 모두 네트워크 트래픽을 전달할 수 있습니다. 이렇게 하면 네트워크에서 로드 밸런싱을 구성할 수 있습니다. 액티브/액티브 장애 조치는 다중 컨텍스트 모드에서 실행되는 유닛에서만 사용할 수 있습니다. 액티브/스탠바이 장애 조치의 경우 한 유닛만 트래픽을 전달하고 다른 유닛은 스탠바이 상태로 대기합니다. 액티브/스탠바이 장애 조치는 단일 또는 다중 컨텍스트 모드에서 실행되는 유닛에서 사용할 수 있습니다. 두 장애 조치 구성 모두 상태 저장 또는 상태 비저장(일반) 장애 조치를 지원합니다.

투명 방화벽은 *와이어* 또는 *스텔스 방화벽*과 같은 역할을 *하는 레이어* 2 방화벽이며 연결된 디바이스에 대한 라우터 홉으로 보이지 않습니다. 보안 어플라이언스는 내부 및 외부 포트에서 동일한 네트워크를 연결합니다. 방화벽은 라우팅 홉이 아니므로 기존 네트워크에 투명 방화벽을 쉽게 도입할 수 있습니다. IP를 재구성할 필요가 없습니다. 기본 라우팅 방화벽 모드 또는 투명 방화벽 모드에서 실행되도록 Adaptive Security Appliance를 설정할 수 있습니다. 모드를 변경할 때 Adaptive Security Appliance는 두 모드 모두에서 지원되지 않는 명령이 많으므로 컨피그레이션을 지웁니다. 이미 채워진 컨피그레이션이 있는 경우 모드를 변경하기 전에 이 컨피그레이션을 백업해야 합니다. 새 컨피그레이션을 생성할 때 이 백업 컨피그레이션을 참조할 수 있습니다. 투명 모드의 방화벽 어플라이언스 컨피그레이션에 대한 자세한 내용은 투명 방화벽 컨피그레이션 예를 참조하십시오.

이 문서에서는 ASA 보안 어플라이언스에서 투명 모드에서 액티브/스탠바이 장애 조치를 구성하는 방법에 대해 중점적으로 설명합니다.

참고: 다중 컨텍스트 모드에서 실행되는 유닛에서는 VPN 장애 조치가 지원되지 않습니다. VPN 장애 조치는 **액티브/스탠바이 장애 조치** 컨피그레이션에만 사용할 수 있습니다.

Cisco에서는 장애 조치에 관리 인터페이스를 사용하지 않는 것이 좋습니다. 특히 보안 어플라이언스가 한 보안 어플라이언스에서 다른 보안 어플라이언스로 연결 정보를 지속적으로 전송하는 상태 저장 장애 조치에는 이 인터페이스를 사용하지 않는 것이 좋습니다. 장애 조치를 위한 인터페이스는 일반 트래픽을 전달하는 인터페이스와 최소 용량이 같아야 하며, ASA 5540의 인터페이스는 기가비트이지만 관리 인터페이스는 FastEthernet 전용입니다. 관리 인터페이스는 관리 트래픽에만 사

용하도록 설계되고 management0/0으로 지정됩니다. 그러나 **management-only** 명령을 사용하여 모든 인터페이스를 관리 전용 인터페이스로 구성할 수 있습니다. 또한 Management 0/0의 경우 관리 전용 모드를 비활성화하여 인터페이스가 다른 인터페이스처럼 트래픽을 전달할 수 있도록 할 수 있습니다. **management-only** 명령에 대한 자세한 내용은 Cisco Security Appliance 명령 참조 버전 8.0을 참조하십시오.

이 컨피그레이션 가이드는 PIX/ASA 7.x Active/Standby 기술을 간략하게 소개하는 샘플 컨피그레이션을 제공합니다. 이 기술을 기반으로 한 이론에 대한 자세한 내용은 ASA/PIX 명령 참조 설명서를 참조하십시오.

사전 요구 사항

요구 사항

하드웨어 요구 사항

장애 조치 컨피그레이션의 두 유닛에는 동일한 하드웨어 컨피그레이션이 있어야 합니다. 동일한 모델이어야 하며 인터페이스 수와 유형이 동일해야 하며 동일한 양의 RAM이 있어야 합니다.

참고: 두 유닛에는 동일한 크기의 플래시 메모리가 필요하지 않습니다. 장애 조치 컨피그레이션에서 플래시 메모리 크기가 다른 유닛을 사용하는 경우, 플래시 메모리가 작은 유닛에 소프트웨어 이미지 파일 및 컨피그레이션 파일을 수용할 충분한 공간이 있는지 확인하십시오. 그렇지 않으면 플래시 메모리가 큰 유닛에서 플래시 메모리가 작은 유닛으로 컨피그레이션 동기화에 실패합니다.

소프트웨어 요구 사항

장애 조치 컨피그레이션의 두 유닛은 운영 모드(라우팅 또는 투명, 단일 또는 다중 컨텍스트)여야 합니다. 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 동일해야 하지만, 업그레이드 프로세스 내에서 다른 버전의 소프트웨어를 사용할 수 있습니다. 예를 들어, 한 유닛을 버전 7.0(1)에서 버전 7.0(2)으로 업그레이드하고 장애 조치가 활성 상태로 유지되도록 할 수 있습니다. Cisco에서는 장기적인 호환성을 보장하기 위해 두 유닛을 모두 동일한 버전으로 업그레이드할 것을 권장합니다.

장애 조치 쌍에서 소프트웨어를 업그레이드하는 방법에 대한 자세한 내용은 *Cisco Security Appliance Command Line Configuration Guide, Version 8.0*의 Performing Zero Downtime Upgrades for Failover Pairs 섹션을 참조하십시오.

라이센스 요구 사항

ASA 보안 어플라이언스 플랫폼에서 하나 이상의 유닛에 **제한(UR) 라이센스가** 있어야 합니다.

참고: 추가 기능 및 혜택을 얻으려면 장애 조치 쌍의 라이센스를 업그레이드해야 할 수 있습니다. 자세한 내용은 장애 조치 쌍의 라이센스 키 업그레이드를 참조하십시오.

참고: 장애 조치에 참여하는 두 보안 어플라이언스의 라이센스 기능(예: SSL VPN 피어 또는 보안 컨텍스트)은 동일해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 7.x 버전 이상의 ASA Security Appliance

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 다음 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- 7.x 버전 이상의 PIX Security Appliance

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

액티브/스탠바이 장애 조치

이 섹션에서는 액티브/스탠바이 장애 조치에 대해 설명하며 다음 항목을 포함합니다.

액티브/스탠바이 장애 조치 개요

액티브/스탠바이 장애 조치를 사용하면 스탠바이 보안 어플라이언스를 사용하여 실패한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛에 장애가 발생하면 스탠바이 상태로 변경되고 스탠바이 유닛은 액티브 상태로 변경됩니다. 액티브 유닛이 되는 유닛은 IP 주소를 가정하고, 투명 방화벽의 경우, 장애가 발생한 유닛의 관리 IP 주소 및 MAC 주소를 가정하고 트래픽을 전달하기 시작합니다. 현재 스탠바이 상태에 있는 유닛은 스탠바이 IP 주소와 MAC 주소를 인수합니다. 네트워크 디바이스는 MAC에서 IP 주소 페어링에서 아무런 변화가 없으므로, 네트워크의 어느 곳에서나 ARP 엔트리가 변경되거나 시간 초과되지 않습니다.

참고: 다중 컨텍스트 모드의 경우 보안 어플라이언스는 모든 컨텍스트를 포함하는 전체 유닛을 장애 조치할 수 있지만 개별 컨텍스트를 개별적으로 장애 조치할 수는 없습니다.

기본/보조 상태 및 활성/대기 상태

장애 조치 쌍의 두 유닛 간의 주요 차이점은 어느 유닛이 액티브 유닛이고 어떤 유닛이 스탠바이 유닛인지, 즉 어떤 IP 주소를 사용해야 하는지, 어떤 유닛이 기본 유닛이고 트래픽을 능동적으로 전달하는 것과 관련이 있습니다.

컨피그레이션에 지정된 대로 유닛이 기본 유닛인 유닛과 보조 유닛 간에 몇 가지 차이가 있습니다.

- 두 유닛이 동시에 시작되며 작동 상태가 동일하면 기본 유닛은 항상 활성 유닛이 됩니다.
- 기본 유닛 MAC 주소는 항상 활성 IP 주소와 결합됩니다. 이 규칙의 예외는 보조 유닛이 활성 상태이며 장애 조치 링크를 통해 기본 MAC 주소를 가져올 수 없을 때 발생합니다. 이 경우 보조

MAC 주소가 사용됩니다.

디바이스 초기화 및 컨피그레이션 동기화

컨피그레이션 동기화는 장애 조치 쌍의 디바이스 중 하나 또는 둘 다 부팅할 때 발생합니다. 컨피그레이션은 항상 액티브 유닛에서 스탠바이 유닛으로 동기화됩니다. 스탠바이 유닛이 초기 시작을 완료하면, 액티브 유닛과 통신하는 데 필요한 장애 조치 명령을 제외하고 실행 중인 컨피그레이션이 지워지며, 액티브 유닛은 전체 컨피그레이션을 스탠바이 유닛으로 전송합니다.

활성 유닛은 다음 항목에 의해 결정됩니다.

- 유닛이 부팅되고 이미 활성으로 작동하는 피어를 탐지하면 스탠바이 유닛이 됩니다.
- 디바이스가 부팅되고 피어를 탐지하지 못하면 활성 유닛이 됩니다.
- 두 유닛이 동시에 부팅되면 기본 유닛이 액티브 유닛이 되고 보조 유닛이 스탠바이 유닛이 됩니다.

참고: 보조 유닛이 부팅되고 기본 유닛이 검색되지 않으면 액티브 유닛이 됩니다. 활성 IP 주소에 고유한 MAC 주소를 사용합니다. 기본 유닛을 사용할 수 있게 되면 보조 유닛에서는 MAC 주소를 기본 유닛의 주소로 변경하며, 네트워크 트래픽이 중단될 수 있습니다. 이를 방지하려면 가상 MAC 주소로 장애 조치 쌍을 구성합니다. 자세한 내용은 이 문서의 액티브/스탠바이 장애 조치 구성 섹션을 참조하십시오.

복제가 시작되면 액티브 유닛의 보안 어플라이언스 콘솔에 Beginning configuration replication:(`:)` 메시지가 `. Sending to mate`(으로 전송)가 완료되면 보안 어플라이언스는 `End Configuration Replication to mate` 메시지를 `.` 복제 내에서 액티브 유닛에 입력된 명령은 스탠바이 유닛에 제대로 복제할 수 없으며, 액티브 유닛에서 복제된 컨피그레이션에 의해 스탠바이 유닛에 입력된 명령을 덮어쓸 수 있습니다. 컨피그레이션 복제 프로세스 내의 장애 조치 쌍에서 유닛에 명령을 입력하지 마십시오. 컨피그레이션 크기에 따라 복제가 몇 초에서 몇 분 정도 걸릴 수 있습니다.

보조 유닛에서 기본 유닛에서 동기화할 때 복제 메시지를 관찰할 수 있습니다.

```
ASA> .

        Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.

ASA>
```

스탠바이 유닛에서는 컨피그레이션이 실행 중인 메모리에만 존재합니다. 동기화 후 컨피그레이션을 플래시 메모리에 저장하려면 다음 명령을 입력합니다.

- 단일 컨텍스트 모드의 경우 액티브 유닛에서 **copy running-config startup-config** 명령을 입력합니다. 이 명령은 스탠바이 유닛에 복제되며, 이 유닛에서는 컨피그레이션을 플래시 메모리에 계속 기록합니다.
- 다중 컨텍스트 모드의 경우 시스템 실행 공간 및 디스크의 각 컨텍스트 내에서 활성 유닛에 **copy running-config startup-config** 명령을 입력합니다. 이 명령은 스탠바이 유닛에 복제되며, 이 유닛에서는 컨피그레이션을 플래시 메모리에 계속 기록합니다. 외부 서버의 시작 컨피그레이션이 있는 컨텍스트는 네트워크를 통해 한 유닛에서 액세스할 수 있으며 각 유닛에 대해 별도로 저장할 필요가 없습니다. 또는 디스크의 컨텍스트를 액티브 유닛에서 외부 서버로 복사한 다음, 디바이스가 다시 로드될 때 사용할 수 있는 스탠바이 유닛의 디스크에 복사할 수 있습니다.

명령 복제

명령 복제는 항상 활성 유닛에서 대기 유닛으로 이동합니다. 액티브 유닛에 명령을 입력하면 장애 조치 링크를 통해 스탠바이 유닛으로 전송됩니다. 명령을 복제하기 위해 활성 컨피그레이션을 플래시 메모리에 저장할 필요가 없습니다.

참고: 스탠바이 유닛에서 변경한 내용은 액티브 유닛에 복제되지 않습니다. 스탠바이 유닛에서 명령을 입력하면 보안 어플라이언스에 `**** WARNING **** Configuration Replication is not performed from Standby unit to Active unit`(스탠바이 유닛에서 액티브 유닛으로 컨피그레이션 복제가) 메시지 . 구성이 더 이상 동기화되지 않습니다. 컨피그레이션에 영향을 미치지 않는 명령을 입력해도 이 메시지가 표시됩니다.

액티브 유닛에 **write standby** 명령을 입력하면 스탠바이 유닛은 실행 중인 컨피그레이션을 지웁니다. 단, 액티브 유닛과 통신하는 데 사용되는 장애 조치 명령은 제외하며, 액티브 유닛은 전체 컨피그레이션을 스탠바이 유닛으로 전송합니다.

다중 컨텍스트 모드의 경우 시스템 실행 공간에서 **write standby** 명령을 입력하면 모든 컨텍스트가 복제됩니다. 컨텍스트 내에서 write standby 명령을 입력하면 이 명령은 컨텍스트 컨피그레이션만 복제합니다.

복제된 명령은 실행 중인 컨피그레이션에 저장됩니다. 복제된 명령을 스탠바이 유닛의 플래시 메모리에 저장하려면 다음 명령을 입력합니다.

- 단일 컨텍스트 모드의 경우 액티브 유닛에서 **copy running-config startup-config** 명령을 입력합니다. 이 명령은 스탠바이 유닛에 복제되며, 이 유닛에서는 컨피그레이션을 플래시 메모리에 계속 기록합니다.
- 다중 컨텍스트 모드의 경우 시스템 실행 공간 및 디스크의 각 컨텍스트 내에서 활성 유닛에 **copy running-config startup-config** 명령을 입력합니다. 이 명령은 스탠바이 유닛에 복제되며, 이 유닛에서는 컨피그레이션을 플래시 메모리에 계속 기록합니다. 외부 서버의 시작 컨피그레이션이 있는 컨텍스트는 네트워크를 통해 한 유닛에서 액세스할 수 있으며 각 유닛에 대해 별도로 저장할 필요가 없습니다. 또는 디스크의 컨텍스트를 액티브 유닛에서 외부 서버로 복사한 다음 스탠바이 유닛의 디스크에 복사할 수 있습니다.

장애 조치 트리거

다음 이벤트 중 하나가 발생하면 유닛이 실패할 수 있습니다.

- 장치에 하드웨어 장애 또는 전원 장애가 있습니다.
- 장치에 소프트웨어 오류가 있습니다.
- 너무 많은 모니터링된 인터페이스에 오류가 발생했습니다.
- 액티브 유닛에 **no failover active** 명령을 입력하거나 **failover active** 명령을 스탠바이 유닛에 입력합니다.

장애 조치 작업

액티브/스탠바이 장애 조치에서는 유닛별로 장애 조치가 발생합니다. 다중 컨텍스트 모드에서 실행되는 시스템에서도 개별 또는 컨텍스트 그룹을 장애 조치할 수 없습니다.

이 표에서는 각 실패 이벤트에 대한 장애 조치 작업을 보여 줍니다. 각 오류 이벤트에 대해 테이블에는 장애 조치 정책(장애 조치 또는 장애 조치 없음), 액티브 유닛에서 수행한 작업, 스탠바이 유닛에

서 수행한 작업, 장애 조치 조건 및 작업에 대한 특별 참고 사항이 표시됩니다. 이 표에서는 장애 조치 동작을 보여 줍니다.

실패 이벤트	정책	활성 작업	대기 작업	참고
액티브 유닛 실패(전원 또는 하드웨어)	장애조치	해당 없음	활성 상태가 됨; 활성을 실패로 표시	모니터링되는 인터페이스 또는 장애 조치 링크에서 hello 메시지가 수신되지 않습니다.
이전에 활성 유닛 복구	장애조치없음	대기 상태가 됨	작업 없음	없음
스탠바이 유닛 실패(전원 또는 하드웨어)	장애조치없음	스탠바이가 실패한 것으로 표시	해당 없음	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛은 인터페이스 오류 임계값을 넘은 경우에도 장애 조치를 시도하지 않습니다.
작업 내에서 장애 조치(failover) 링크 실패	장애조치없음	장애 조치 인터페이스를 실패한 것으로 표시	장애 조치 인터페이스를 실패한 것으로 표시	장애 조치 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치를 수행할 수 없으므로 최대한 빨리 장애 조치 링크를 복원해야 합니다.
시작 시 장애 조치 링크 실패	장애조치없음	장애 조치 인터페이스를 실패한 것으로 표시	활성 상태가 됨	시작 시 장애 조치 링크가 다운되면 두 유닛 모두 액티브 상태가 됩니다.
상태 저장 장애 조치 링크 실패	장애조치없음	작업 없음	작업 없음	상태 정보가 오래되고 장애 조치가 발생하면 세션이 종료됩니다.
임계값을 초과하는 활성 유닛에서 인터페이스 오류 발생	장애조치	활성으로 실패 표시	활성 상태가 됨	없음
임계값을 초과하는 스탠바이 유닛에서 인터페이	장애조치없	작업 없음	스탠바이가 실패한 것으로 표시	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 인터페이스 실패 임계값을 넘은 경우에도 장애 조치를 시

스 오류 발생	음			도하지 않습니다.

일반 및 상태 기반 장애 조치

보안 어플라이언스는 두 가지 유형의 장애 조치(일반 및 상태 저장)를 지원합니다. 이 섹션에서는 다음 항목을 다룹니다.

- 일반 장애 조치
- 상태 기반 장애 조치

일반 장애 조치

장애 조치가 발생하면 모든 활성 연결이 삭제됩니다. 클라이언트는 새 활성 유닛이 인계될 때 연결을 다시 설정해야 합니다.

상태 기반 장애 조치

상태 저장 장애 조치가 활성화되면 활성 유닛은 연결 당 상태 정보를 대기 유닛에 지속적으로 전달합니다. 장애 조치가 발생하면 새 액티브 유닛에서 동일한 연결 정보를 사용할 수 있습니다. 지원되는 최종 사용자 애플리케이션은 동일한 통신 세션을 유지하기 위해 다시 연결할 필요가 없습니다.

스탠바이 유닛에 전달되는 상태 정보에는 다음이 포함됩니다.

- NAT 변환 테이블
- TCP 연결 상태
- UDP 연결 상태
- ARP 테이블
- 레이어 2 브리지 테이블(방화벽이 **투명 방화벽** 모드에서 실행되는 경우에만)
- HTTP 연결 상태(HTTP 복제가 활성화된 경우)
- ISAKMP 및 IPSec SA 테이블
- GTP PDP 연결 데이터베이스

상태 저장 장애 조치가 활성화된 경우 스탠바이 유닛에 전달되지 않는 정보에는 다음이 포함됩니다.

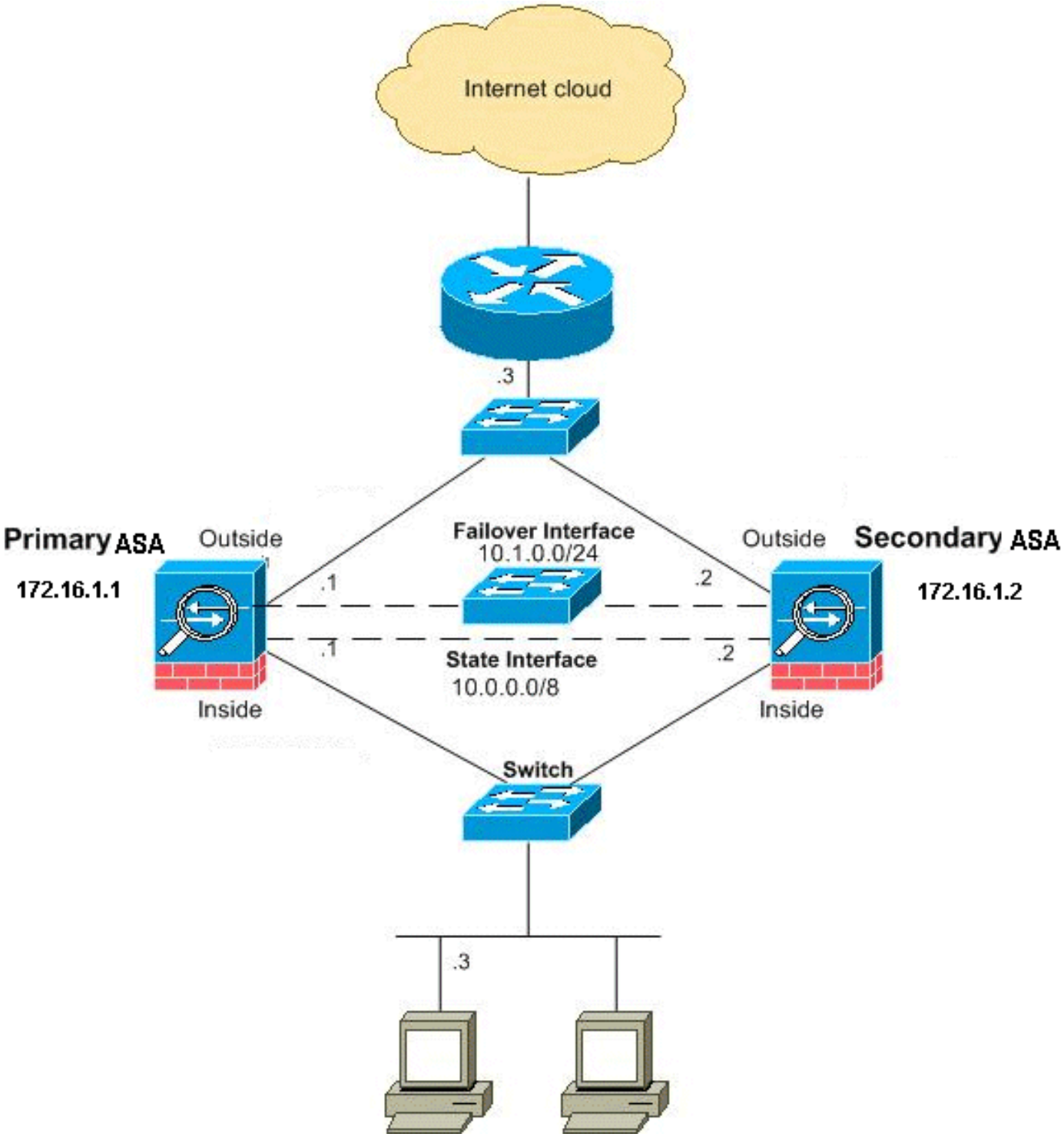
- HTTP 연결 테이블(HTTP 복제가 활성화된 경우 제외)
- 사용자 인증(uauth) 테이블
- 라우팅 테이블
- 보안 서비스 모듈에 대한 상태 정보

참고: 활성 Cisco IP SoftPhone 세션 내에서 장애 조치가 발생하면 통화 세션 상태 정보가 대기 유닛에 복제되므로 통화가 활성 상태로 유지됩니다. 통화가 종료되면 IP SoftPhone 클라이언트가 Cisco CallManager와의 연결이 끊깁니다. 이는 스탠바이 유닛에 CTIQBE 끊기 메시지에 대한 세션 정보가 없기 때문에 발생합니다. IP SoftPhone 클라이언트가 특정 기간 내에 Cisco CallManager로부터 응답을 받지 못하면 Cisco CallManager에 연결할 수 없는 것으로 간주하여 자체적으로 등록을 취소합니다.

LAN 기반 액티브/스탠바이 장애 조치 구성

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 섹션에서는 이더넷 장애 조치 링크를 사용하여 투명 모드에서 액티브/스탠바이 장애 조치를 구성하는 방법에 대해 설명합니다. LAN 기반 장애 조치를 구성할 때 보조 디바이스가 기본 디바이스에서 실행 중인 컨피그레이션을 가져오려면 먼저 보조 디바이스를 부트스트랩하여 장애 조치 링크를 인식해야 합니다.

참고: 케이블 기반 장애 조치에서 LAN 기반 장애 조치로 변경하는 경우 케이블 기반 장애 조치 컨피그레이션에 대해 완료한 각 인터페이스에 대한 활성 및 대기 IP 주소 할당과 같은 여러 단계를 건너뛸 수 있습니다.

기본 유닛 컨피그레이션

LAN 기반 액티브/스탠바이 장애 조치 컨피그레이션에서 기본 유닛을 구성하려면 다음 단계를 완료합니다. 이러한 단계는 기본 유닛에서 장애 조치를 활성화하는 데 필요한 최소 컨피그레이션을 제공합니다. 다중 컨텍스트 모드의 경우, 달리 명시되지 않는 한 모든 단계가 시스템 실행 영역에서 수행됩니다.

액티브/스탠바이 장애 조치 쌍에서 기본 유닛을 구성하려면 다음 단계를 완료하십시오.

1. 아직 수행하지 않은 경우 관리 인터페이스(투명 모드)에 대한 활성 및 대기 IP 주소를 구성합니다. 대기 IP 주소는 현재 대기 유닛인 보안 어플라이언스에서 사용됩니다. 활성 IP 주소와 동일한 서브넷에 있어야 합니다.**참고:** 전용 상태 저장 장애 조치 인터페이스를 사용하는 경우 상태 저장 장애 조치 링크에 대한 IP 주소를 구성하지 마십시오. 나중에 failover **interface ip** 명령을 사용하여 전용 상태 기반 장애 조치 인터페이스를 구성합니다.
   ```
   hostname(config-if)#ip address active_addr netmask
                           standby standby_addr
   ```

   각 인터페이스에 IP 주소가 필요한 라우팅 모드와 달리 투명 방화벽에는 전체 디바이스에 할당된 IP 주소가 있습니다. 보안 어플라이언스는 이 IP 주소를 시스템 메시지 또는 AAA 통신 등 보안 어플라이언스에서 시작되는 패킷의 소스 주소로 사용합니다. 이 예에서는 기본 ASA의 IP 주소가 아래와 같이 구성됩니다.
   ```
   hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
   ```

   여기서 172.16.1.1은 기본 유닛에 사용되며 보조(스탠바이) 유닛에 172.16.1.2 할당됩니다.**참고:** 다중 컨텍스트 모드에서는 각 컨텍스트 내에서 인터페이스 주소를 구성해야 합니다. 컨텍스트 간으로 전환하려면 changeto context 명령을 사용합니다. 명령 프롬프트가 hostname`/context(config-if)#`으로 변경됩니다. 여기서 context는 현재 컨텍스트의 이름입니다.
2. (PIX 보안 어플라이언스 플랫폼에만 해당) LAN 기반 장애 조치를 활성화합니다.
   ```
   hostname(config)#failover lan enable
   ```

3. 유닛을 기본 유닛으로 지정합니다.
   ```
   hostname(config)#failover lan unit primary
   ```

4. 장애 조치 인터페이스를 정의합니다.장애 조치 인터페이스로 사용할 인터페이스를 지정합니다.
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   이 설명서에서는 장애 조치 인터페이스에 "failover"(Ethernet0의 인터페이스 이름)가 사용됩니다.
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   if_*name* 인수는 phy_*if* 인수에 지정된 인터페이스에 이름을 할당합니다. phy_*if* 인수는 Ethernet1과 같은 물리적 포트 이름이나 이전에 생성한 하위 인터페이스(예: Ethernet0/2.3)이 될 수 있습니다.장애 조치 링크에 액티브 및 스탠바이 IP 주소 할당
   ```
   hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
   ```

   이 설명서에서 장애 조치 링크를 구성하려면 액티브 유닛에 10.1.0.1이 사용되고, 스탠바이 유닛에 10.1.0.2이 사용되며, "failover"는 Ethernet0의 인터페이스 이름입니다.
   ```
   hostname(config)#failover interface ip failover 10.1.0.1
                           255.255.255.0 standby 10.1.0.2
   ```

대기 IP 주소는 활성 IP 주소와 동일한 서브넷에 있어야 합니다. 스탠바이 주소 서브넷 마스크를 식별할 필요가 없습니다.장애 조치 링크 IP 주소 및 MAC 주소는 장애 조치 시 변경되지 않습니다. 장애 조치 링크의 활성 IP 주소는 항상 기본 유닛에 유지되며, 대기 IP 주소는 보조 유닛에 유지됩니다.인터페이스 활성화

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

이 예에서는 Ethernet3가 장애 조치에 사용됩니다.

```
hostname(config)#interface ethernet3

hostname(config-if)#no shutdown
```

5. (선택 사항) 상태 기반 장애 조치를 활성화하려면 상태 기반 장애 조치 링크를 구성합니다.상태 기반 장애 조치 링크로 사용할 인터페이스를 지정합니다.

```
hostname(config)#failover link if_name phy_if
```

이 예에서는 Ethernet2의 인터페이스 이름으로 "state"를 사용하여 장애 조치 링크 상태 정보를 교환했습니다.

```
hostname(config)#failover link state Ethernet2
```

참고: 상태 저장 장애 조치 링크가 장애 조치 링크 또는 데이터 인터페이스를 사용하는 경우 *if_name* ***인수***를 제공하기만 하면 됩니다.if *_name* ***인수***는 phy_if **인수**에 지정된 인터페이스에 논리 이름을 **할당합니다**. phy_*if* ***인수***는 Ethernet1과 같은 물리적 포트 이름 또는 이전에 생성한 Ethernet0/2.3 같은 하위 인터페이스가 될 수 있습니다. 이 인터페이스는 대체작동 링크로 사용할 수 있는 경우를 제외하고 다른 용도로 사용할 수 없습니다.상태 저장 장애 조치 링크에 활성 및 대기 IP 주소를 할당합니다.**참고: 상태** 저장 장애 조치 링크가 장애 조치 링크 또는 데이터 인터페이스를 사용하는 경우 이 단계를 건너뜁니다. 인터페이스에 대한 액티브 및 스탠바이 IP 주소를 이미 정의했습니다.

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

이 예에서 10.0.0.1은 활성 및 10.0.0.2은 상태 저장 장애 조치 링크의 대기 IP 주소로 사용됩니다.

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                      standby 10.0.0.2
```

대기 IP 주소는 활성 IP 주소와 동일한 서브넷에 있어야 합니다. 스탠바이 주소 서브넷 마스크를 식별할 필요가 없습니다.상태 저장 장애 조치 링크 IP 주소 및 MAC 주소는 데이터 인터페이스를 사용하지 않는 한 장애 조치 시 변경되지 않습니다. 활성 IP 주소는 항상 기본 유닛에 있고 대기 IP 주소는 보조 유닛에 유지됩니다.인터페이스를 활성화합니다.**참고: 상태** 저장 장애 조치 링크가 장애 조치 링크 또는 데이터 인터페이스를 사용하는 경우 이 단계를 건너뜁니다. 이미 인터페이스를 활성화했습니다.

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

참고: 예를 들어, 이 시나리오에서는 상태 저장 장애 조치 링크에 Ethernet2가 사용됩니다.

```
hostname(config)#interface ethernet2

hostname(config-if)#no shutdown
```

6. 장애 조치를 활성화합니다.
   ```
   hostname(config)#failover
   ```

   참고: 먼저 기본 디바이스에서 failover 명령을 실행한 다음 보조 디바이스에서 실행합니다. 보조 디바이스에서 failover 명령을 실행하면 보조 디바이스에서 즉시 기본 디바이스에서 컨피그레이션을 가져오고 자신을 *대기*로 설정합니다. 기본 ASA는 작동 상태를 유지하고 트래픽을 정상적으로 전달하며 자신을 *활성* 디바이스로 표시합니다. 이 시점부터 활성 디바이스에서 장애가 발생할 때마다 대기 디바이스가 활성 상태로 표시됩니다.
7. 시스템 컨피그레이션을 플래시 메모리에 저장합니다.
   ```
   hostname(config)#copy running-config startup-config
   ```

보조 유닛 컨피그레이션

보조 유닛에 필요한 유일한 컨피그레이션은 장애 조치 인터페이스를 위한 것입니다. 보조 유닛에서는 기본 유닛과 처음 통신하기 위해 이러한 명령이 필요합니다. 기본 유닛에서 보조 유닛으로 컨피그레이션을 전송한 후 두 컨피그레이션의 유일한 영구적인 차이점은 failover **lan unit** 명령이며, 각 유닛을 기본 또는 보조 유닛으로 식별합니다.

다중 컨텍스트 모드의 경우 달리 명시되지 않는 한 모든 단계가 시스템 실행 영역에서 수행됩니다.

보조 유닛을 구성하려면 다음 단계를 완료합니다.

1. (PIX 보안 어플라이언스 플랫폼에만 해당) LAN 기반 장애 조치를 활성화합니다.
   ```
   hostname(config)#failover lan enable
   ```

2. 장애 조치 인터페이스를 정의합니다. 기본 유닛에 사용한 것과 동일한 설정을 사용합니다.장애 조치 인터페이스로 사용할 인터페이스를 지정합니다.
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   이 설명서에서 Ethernet0은 LAN 장애 조치 인터페이스에 사용됩니다.
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   if_*name* 인수는 phy_*if* 인수에 지정된 인터페이스에 이름을 할당합니다.장애 조치 링크에 액티브 및 스탠바이 IP 주소를 할당합니다.
   ```
   hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
   ```

   이 설명서에서 장애 조치 링크를 구성하려면 액티브 유닛에 10.1.0.1이 사용되고, 스탠바이 유닛에 10.1.0.2이 사용되며, "failover"는 Ethernet0의 인터페이스 이름입니다.
   ```
   hostname(config)#failover interface ip failover 10.1.0.1
                        255.255.255.0 standby 10.1.0.2
   ```

   참고: 기본 유닛에서 장애 조치 인터페이스를 구성할 때 기본 유닛에서 입력한 것과 정확히 동일하게 이 명령을 입력합니다.인터페이스를 활성화합니다.
   ```
   hostname(config)#interface phy_if

   hostname(config-if)#no shutdown
   ```

   예를 들어 이 시나리오에서는 Ethernet0이 장애 조치에 사용됩니다.
   ```
   hostname(config)#interface ethernet3
   ```

```
hostname(config-if)#no shutdown
```

3. (선택 사항) 이 유닛을 보조 유닛으로 지정합니다.
```
hostname(config)#failover lan unit secondary
```

참고: 이 단계는 기본적으로 유닛이 이전에 구성되지 않은 경우 보조로 지정되므로 선택 사항입니다.

4. 장애 조치를 활성화합니다.
```
hostname(config)#failover
```

참고: 장애 조치를 활성화한 후 활성 유닛은 실행 중인 메모리의 컨피그레이션을 스탠바이 유닛으로 전송합니다. 컨피그레이션이 동기화되면 Beginning configuration *replication*(컨피그레이션 *복제 시작)* 메시지가 *표시됩니다. Sending to mate* and *End Configuration Replication to mate*는 액티브 유닛 콘솔에 나타납니다.

5. 실행 중인 컨피그레이션이 복제를 완료한 후 컨피그레이션을 플래시 메모리에 저장합니다.
```
hostname(config)#copy running-config startup-config
```

구성

이 문서에서는 다음 구성을 사용합니다.

기본 ASA

```
ASA#show running-config
 ASA Version 7.2(3)
!
!--- To set the firewall mode to transparent mode, !---
use the firewall transparent command !--- in global
configuration mode.

firewall transparent
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif failover

  description LAN Failover Interface
!
interface Ethernet1
 nameif inside
 security-level 100
!
interface Ethernet2
 nameif outside
 security-level 0

!--- Configure no shutdown in the stateful failover
interface !--- of both Primary and secondary ASA.

interface Ethernet3
 nameif state
 description STATE Failover Interface
!
```

```
interface Ethernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Assign the IP address to the Primary and !---
Seconday ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2

failover
failover lan unit primary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover link state Ethernet3
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
failover interface ip state 10.0.0.1 255.0.0.0 standby
10.0.0.2

asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
```

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

보조 ASA

```
ASA#show running-config
ASA Version 7.2(3)
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
failover
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

다음을 확인합니다.

show failover 명령 사용

이 섹션에서는 show failover 명령 출력에 대해 설명합니다. 각 유닛에서 **show failover** 명령을 사용하여 장애 조치 상태를 확인할 수 있습니다.

기본 ASA

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
```

```
Last Failover at: 00:08:03 UTC Jan 1 1993
        This host: Primary - Active
                Active time: 1820 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         185        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7012
        Xmit Q:         0       1       185
```

보조 ASA

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 16:39:12 UTC Aug 9 2009
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Active time: 1871 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         183        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    0          0          0          0
        Xlate_Timeout   0          0          0          0
```

```
        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7043
        Xmit Q:         0       1       183
```

상태를 확인하려면 **show failover state** 명령을 사용합니다.

기본 ASA

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             00:02:36 UTC Jan 1 1993

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

보조 유닛

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set
```

장애 조치 유닛의 IP 주소를 확인하려면 **show failover interface** 명령을 사용합니다.

기본 유닛

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.1
                Other IP Address : 10.1.0.2
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.1
                Other IP Address : 10.0.0.2
```

보조 유닛

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.2
                Other IP Address : 10.1.0.1
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.2
                Other IP Address : 10.0.0.1
```

모니터링되는 인터페이스 보기

모니터링되는 인터페이스의 상태를 보려면 단일 컨텍스트 모드에서 **글로벌 컨피그레이션 모드**에서 show monitor-interface 명령을 입력합니다. 다중 컨텍스트 모드에서 컨텍스트 내에서 **show monitor-interface**를 입력합니다.

기본 ASA

```
ASA(config)#show monitor-interface
        This host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

보조 ASA

```
ASA(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
```

참고: 장애 조치 IP 주소를 입력하지 않으면 IP 주소에 대해 show failover 명령이 0.0.0.0 표시되고 인터페이스 모니터링은 *대기* 상태로 *유지됩니다*. 다른 장애 조치 상태에 대한 자세한 내용은 *Cisco Security Appliance Command Reference, Version 7.2*의 show failover 섹션을 참조하십시오.

실행 중인 컨피그레이션에서 장애 조치 명령 표시

실행 중인 컨피그레이션에서 failover 명령을 보려면 다음 명령을 입력합니다.

```
hostname(config)#show running-config failover
```

모든 failover 명령이 표시됩니다. 다중 컨텍스트 모드에서 실행되는 유닛의 경우 시스템 실행 공간에 **show running-config failover** 명령을 입력합니다. 실행 중인 컨피그레이션에 failover 명령을 표시하고 기본값을 변경하지 않은 명령을 포함하려면 **show running-config all failover** 명령을 입력합니다.

장애 조치 기능 테스트

장애 조치 기능을 테스트하려면 다음 단계를 완료하십시오.

1. 액티브 유닛 또는 장애 조치 그룹이 FTP를 통해 예상한 대로 트래픽을 전달하여 다른 인터페이스의 호스트 간에 파일을 전송하는지 테스트합니다.
2. 다음 명령을 사용하여 스탠바이 유닛에 장애 조치를 강제로 적용합니다.액티브/스탠바이 장애 조치의 경우 액티브 유닛에서 다음 명령을 입력합니다.
   ```
   hostname(config)#no failover active
   ```
3. 동일한 두 호스트 간에 다른 파일을 보내려면 FTP를 사용합니다.

4. 테스트가 성공하지 못한 경우 장애 조치 상태를 확인하려면 **show failover 명령**을 입력합니다.
5. 완료되면 다음 명령을 사용하여 유닛 또는 장애 조치 그룹을 활성 상태로 복원할 수 있습니다 .액티브/스탠바이 장애 조치의 경우 액티브 유닛에서 다음 명령을 입력합니다.

```
hostname(config)#failover active
```

강제 장애 조치

스탠바이 유닛이 액티브 상태가 되도록 하려면 다음 명령 중 하나를 입력합니다.

스탠바이 유닛에서 다음 명령을 입력합니다.

```
hostname#failover active
```

활성 유닛에서 다음 명령을 입력합니다.

```
hostname#no failover active
```

장애 조치(failover) 사용 안 함

장애 조치를 비활성화하려면 다음 명령을 입력합니다.

```
hostname(config)#no failover
```

액티브/스탠바이 쌍에서 장애 조치를 비활성화하면 재시작할 때까지 각 유닛의 액티브 및 스탠바이 상태가 유지됩니다. 예를 들어 스탠바이 유닛은 대기 모드로 유지되므로 두 유닛이 트래픽을 전달하지 않습니다. 스탠바이 유닛을 액티브 상태로 만들려면(장애 조치가 비활성화된 경우에도) Forcing Failover 섹션을 참조하십시오.

액티브/액티브 쌍에서 장애 조치를 비활성화하면 장애 조치 그룹은 현재 활성 상태인 유닛에 관계없이 액티브 상태로 유지됩니다. 어떤 유닛을 선호하든 상관없습니다. 시스템 실행 공간에 **no failover** 명령을 입력할 수 있습니다.

실패한 유닛 복원

오류가 발생한 유닛을 오류가 없는 상태로 복원하려면 다음 명령을 입력합니다.

```
hostname(config)#failover reset
```

오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원하면 자동으로 활성화되지 않습니다. 복원된 유닛 또는 그룹은 장애 조치(강제 또는 자연)에 의해 활성화될 때까지 스탠바이 상태로 유지됩니다. 예외는 preempt 명령으로 구성된 장애 조치 그룹입니다. 이전에 활성 상태였던 경우 장애 조치 그룹은 preempt 명령으로 구성되고 실패한 유닛이 기본 유닛인 경우 액티브 상태가 됩니다.

문제 해결

장애 조치가 발생하면 두 보안 어플라이언스는 시스템 메시지를 전송합니다. 이 섹션에는 다음 항목이 포함됩니다.

장애 조치 모니터링

이 예에서는 장애 조치가 네트워크 인터페이스를 모니터링하기 시작하지 않은 경우 발생하는 상황을 보여 줍니다. 장애 조치는 해당 인터페이스의 다른 유닛에서 두 번째 `hello` 패킷을 듣기 전까지 네트워크 인터페이스를 모니터링하기 시작하지 않습니다. 30초 정도 걸립니다. 디바이스가 STP(Spanning Tree Protocol)를 실행하는 네트워크 스위치에 연결된 경우 스위치에 구성된 시간(일반적으로 15초로 구성되며 이 30초 지연)의 2배가 소요됩니다. 이는 ASA 부팅 시 장애 조치 이벤트 직후 네트워크 스위치가 임시 브리지 루프를 감지하기 때문입니다. 이 루프를 탐지하면 이 루프는 시간 동안 이러한 인터페이스에서 패킷을 전달하도록 중지합니다. 그런 다음 모드로 들어가서 추가적인 시간을 설정합니다. 이 시간 내에 스위치는 브리지 루프를 수신하지만 트래픽을 전달하지 않거나 장애 조치 `hello` 패킷을 전달하지 않습니다. 전달 지연 시간(30초)의 2배가 지나면 트래픽 흐름이 다시 시작됩니다. 각 ASA는 다른 유닛에서 30초 상당의 `hello` 패킷을 수신할 때까지 모드로 유지됩니다. ASA가 트래픽을 전달하는 시간 내에 `hello` 패킷을 수신하지 않기 때문에 다른 유닛에 오류가 발생하지 않습니다. 다른 모든 장애 조치 모니터링은 계속 발생합니다. 즉, 전원, 인터페이스 손실 링크, 장애 조치 케이블 `hello`.

장애 조치의 경우, ASA 인터페이스에 연결하는 모든 스위치 포트에서 portfast를 활성화하는 것이 좋습니다. 또한 이러한 포트에서 채널링 및 트렁킹을 비활성화해야 합니다. ASA의 인터페이스가 장애 조치 내에 다운되면, 포트가 수신 대기에서 전달 모드로 전환되는 동안 30초 동안 기다릴 필요가 없습니다.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

요컨대 장애 조치 문제를 좁히려면 다음 단계를 확인하십시오.

- 인터페이스에 연결된 네트워크 케이블을 대기/실패 상태로 확인하고 가능한 경우 교체합니다.
- 두 유닛 간에 연결된 스위치가 있는 경우 대기/실패 상태의 인터페이스에 연결된 네트워크가 올바르게 작동하는지 확인합니다.
- 인터페이스에 연결된 스위치 포트가 대기/실패 상태로 있는지 확인하고 가능한 경우 스위치의 다른 FE 포트를 사용합니다.
- 인터페이스에 연결된 스위치 포트에서 포트 속도를 높이고 트렁킹 및 채널링을 모두 비활성화

했는지 확인합니다.

유닛 오류

이 예에서는 장애 조치가 오류를 감지했습니다. 기본 유닛의 Interface 1은 장애의 원인입니다. 장애 때문에 유닛이 다시 모드로 돌아옵니다. 실패한 유닛이 네트워크에서 자신을 제거하고(인터페이스가 다운됨) 더 이상 네트워크에서 `hello` 패킷을 보내지 않습니다. 액티브 유닛은 장애가 발생한 유닛이 교체되고 장애 조치 통신이 다시 시작될 때까지 상태로 유지됩니다.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
```

LU 할당 연결 실패

다음 오류 메시지가 표시되면 메모리 문제가 있을 수 있습니다.

```
LU
```

이 문제는 Cisco 버그 ID CSCte80027에 설명되어 있습니다(등록된 고객만 해당). 이 문제를 해결하려면 방화벽을 이 버그가 수정된 소프트웨어 버전으로 업그레이드하십시오. 이 버그가 수정된 ASA 소프트웨어 버전 중 일부는 8.2(4), 8.3(2), 8.4(2)입니다.

장애 조치 시스템 메시지

보안 어플라이언스는 우선 순위 레벨 2에서 장애 조치와 관련된 여러 시스템 메시지를 발급하며, 이는 심각한 상태를 나타냅니다. 이러한 메시지를 보려면 Cisco Security Appliance 로깅 컨피그레이션 및 시스템 로그 메시지를 참조하여 로깅을 활성화하고 시스템 메시지에 대한 설명을 확인하십시오.

참고: 스위치오버 내에서 장애 조치가 논리적으로 종료되고 인터페이스가 실행되어 syslog **411001** 및 **411002** 메시지가 생성됩니다. 이것은 정상적인 활동입니다.

디버그 메시지

디버그 메시지를 보려면 debug fover 명령**을** 입력합니다. 자세한 내용은 Cisco Security Appliance 명령 참조를 참조하십시오.

참고: 디버깅 출력은 CPU 프로세스에 높은 우선 순위가 할당되므로 시스템 성능에 크게 영향을 줄 수 있습니다. 따라서 debug **fover** 명령만 사용하여 특정 문제를 해결하거나 Cisco 기술 지원 담당자와의 문제 해결 세션 내에서만 문제를 해결합니다.

SNMP

장애 조치를 위한 SNMP syslog 트랩을 수신하려면 SNMP 에이전트를 구성하여 SNMP 트랩을 SNMP 관리 스테이션으로 전송하고, syslog 호스트를 정의하고, Cisco syslog MIB를 SNMP 관리 스테이션으로 컴파일합니다. 자세한 내용은 Cisco **Security Appliance 명령 참조**의 **snmp-server** 및 **logging** 명령을 참조하십시오.

장애 조치 폴링 시간

장애 조치 유닛 폴링 및 대기 시간을 지정하려면 전역 컨피그레이션 모드**에서 failover polltime** 명령을 사용합니다.

failover polltime `unit msec [time]` 대기 유닛의 존재를 확인하기 위해 시간 간격을 나타내기 위해 hello 메시지를 폴링합니다.

마찬가지로, failover `holdtime unit msec [time]`은 장애 조치 링크에 대한 hello 메시지를 유닛에서 수신해야 하는 기간 설정을 나타내며, 그 이후에는 피어 유닛이 실패했다고 선언됩니다.

액티브/스탠바이 장애 조치 컨피그레이션에서 데이터 인터페이스 폴링 및 대기 시간을 지정하려면 글로벌 컨피그레이션 모드에서 failover polltime **interface** 명령을 사용합니다. 기본 폴링 및 대기 시간을 복원하려면 이 명령의 **no** 형식을 사용합니다.

failover polltime interface [msec] *time* **[holdtime** *time***]**

데이터 인터페이스에서 hello 패킷이 전송되는 빈도를 변경하려면 failover polltime **interface** 명령을 사용합니다. 이 명령은 액티브/스탠바이 장애 조치에만 사용할 수 있습니다. 액티브/액티브 장애 조치의 경우 failover polltime **interface** 명령 대신 장애 조치 그룹 컨피그레이션 모드에서 polltime interface 명령을 사용합니다.

인터페이스 폴링 시간**의** 5배 미만의 holdtime 값은 입력할 수 없습니다. 더 빠른 폴링 시간을 통해 보안 어플라이언스는 장애를 탐지하고 장애 조치를 더 빠르게 트리거할 수 있습니다. 그러나 더 빠른 탐지를 통해 네트워크가 일시적으로 혼잡할 때 불필요한 전환이 발생할 수 있습니다. 인터페이스 테스트는 대기 시간의 절반 이상 동안 인터페이스에서 hello 패킷이 들리지 않을 때 시작됩니다.

컨피그레이션에 failover polltime unit 및 failover polltime interface 명령을 모두 포함할 수 있습니다.

다음 예에서는 인터페이스 폴링 빈도를 500밀리초로, 보류 시간을 5초로 설정합니다.

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

자세한 내용은 *Cisco* Security Appliance 명령 참조, *버전 7.2의 장애 조치* 폴링 시간 섹션을 참조하십시오.

장애 조치 컨피그레이션에서 인증서/개인 키 내보내기

기본 디바이스는 개인 키/인증서를 보조 유닛에 자동으로 복제합니다. 인증서/개인 키를 포함하는 컨피그레이션을 스탠바이 유닛에 복제하려면 액티브 유닛에서 **write memory** 명령을 실행합니다. 스탠바이 유닛의 모든 키/인증서가 지워지고 액티브 유닛 컨피그레이션에 의해 다시 채워집니다.

참고: 활성 디바이스에서 인증서, 키 및 신뢰 지점을 수동으로 가져온 다음 대기 디바이스로 내보내면 안 됩니다.

경고: 장애 조치(failover) 메시지 암호 해독 실패.

오류 메시지:

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

이 문제는 장애 조치 키 컨피그레이션으로 인해 발생합니다. 이 문제를 해결하려면 장애 조치 키를 제거하고 새 공유 키를 구성하십시오.

문제/장애: 투명 액티브/스탠바이 다중 모드 장애 조치를 구성한 후 장애 조치가 항상 플래핑됩니다.

두 ASA의 내부 인터페이스가 직접 연결되어 있고 두 ASA의 외부 인터페이스가 직접 연결되어 있는 경우 장애 조치는 안정적입니다. 그러나 이 사이에 스위치가 사용될 때 장애 조치가 플래핑됩니다.

해결책: 이 문제를 해결하려면 ASA 인터페이스에서 BPDU를 비활성화합니다.

ASA 모듈 장애 조치

AIP-SSM(Advanced Inspection and Prevention Security Services Module) 또는 CSC-SSM(Content Security and Control Security Services Module)을 액티브 및 스탠바이 유닛에서 사용하는 경우 장애 조치 측면에서 ASA와 독립적으로 작동합니다. **모듈은 액티브 및 스탠바이 유닛에서 수동으로 구성해야 하며, 장애 조치에서는 모듈 컨피그레이션을 복제하지 않습니다.**

장애 조치의 경우 AIP-SSM 또는 CSC-SSM 모듈이 있는 ASA 유닛 모두 하드웨어 유형이 같아야 합니다. 예를 들어 기본 유닛에 ASA-SSM-10 모듈이 있는 경우 보조 유닛에는 ASA-SSM-10 모듈이 있어야 합니다.

장애 조치(failover) 메시지 블록 할당 실패

오류 메시지 `%PIX|ASA-3-105010: ()` .

설명: 블록 메모리가 부족합니다. 이는 일시적인 메시지이며 보안 어플라이언스가 복구되어야 합니다. *기본*은 보조 유닛의 보조 유닛으로 나열될 수도 있습니다.

권장 작업: 현재 블록 메모리를 모니터링하려면 **show blocks** 명령을 사용합니다.

AIP 모듈 장애 조치 문제

장애 조치 컨피그레이션에 두 개의 ASA가 있고 각 ASA에 AIP-SSM이 있는 경우 AIP-SSM의 컨피그레이션을 수동으로 복제해야 합니다. ASA의 컨피그레이션만 장애 조치 메커니즘에 의해 복제됩니다. AIP-SSM은 장애 조치에 포함되지 않습니다.

먼저 AIP-SSM은 장애 조치 측면에서 ASA와 독립적으로 작동합니다. 장애 조치의 경우 ASA 관점에서 필요한 모든 것은 AIP 모듈이 동일한 하드웨어 유형이어야 한다는 것입니다. 그 외에도 다른 장애 조치 부분과 마찬가지로, 액티브 및 스탠바이 간의 ASA 컨피그레이션이 동기화되어야 합니다.

AIP의 셋팅에 관해서, 그들은 효과적으로 독립적인 센서입니다. 둘 사이에는 아무런 장애 조치가 없

으며, 그들은 서로를 인식하지 못한다. 독립 버전의 코드를 실행할 수 있습니다. 즉, ASA는 장애 조치와 관련하여 AIP의 코드 버전을 고려하지 않습니다.

ASDM은 AIP에서 구성한 관리 인터페이스 IP를 통해 AIP에 대한 연결을 시작합니다. 즉, 일반적으로 HTTPS를 통해 센서에 연결되며, 이는 센서 설정 방법에 따라 달라집니다.

IPS(AIP) 모듈과 독립적으로 ASA의 페일오버를 가질 수 있습니다. 관리 IP에 연결되므로 여전히 동일한 IP에 연결되어 있습니다. 다른 AIP에 연결하려면 관리 IP에 다시 연결하여 이를 구성하고 액세스해야 합니다.

ASA 참조: Cisco ASA 5500 Series ASA(Adaptive Security Appliance)를 통해 AIP-SSM(Advanced Inspection and Prevention Security Services Module)으로 전달되는 네트워크 트래픽을 전송하는 방법에 대한 자세한 내용과 샘플 컨피그레이션을 보려면 ASA에서 AIP SSM 컨피그레이션 예로 네트워크 트래픽 보내기

알려진 문제

버전 8.x 소프트웨어를 사용하는 보조 ASA의 ASDM에 액세스하려고 시도하면 장애 조치 컨피그레이션을 위해 ASDM 버전 6.x에 액세스하려고 하면 다음 오류가 발생합니다.

: .

인증서에서 Issuer(발급자) 및 Subject Name(주체 이름)은 *스탠바이* 유닛의 IP 주소가 아닌 *활성* 유닛의 IP 주소입니다.

ASA 버전 8.x에서 내부(ASDM) 인증서가 액티브 유닛에서 스탠바이 유닛으로 복제되어 오류 메시지가 나타납니다. 그러나 동일한 방화벽이 5.x ASDM의 버전 7.x 코드에서 실행되며 ASDM에 액세스하려고 하면 다음과 같은 정기적인 보안 경고가 표시됩니다.

.

인증서를 확인하면 발급자 및 주체 이름은 스탠바이 유닛의 IP 주소입니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco PIX 방화벽 소프트웨어
- FWSM(Firewall Services Module) 장애 조치 컨피그레이션
- FWSM 장애 조치 문제 해결
- Cisco Secure PIX Firewall에서 장애 조치가 작동하는 방식
- 기술 지원 및 문서 – Cisco Systems