FWSM 기본 컨피그레이션 예

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
관련 제품
표기 규칙
배경 정보
구성
네트워크 다이어그램
구성
다음을 확인합니다.
문제 해결
문제/장애:FWSM에서 IPS 센서 4270으로 VLAN 트래픽을 전달할 수 없습니다.
솔루션
FWSM에서 Out-Of-Order 패킷 문제
솔루션
문제/장애:비대칭 라우팅 패킷을 방화벽을 통해 전달할 수 없습니다.
솔루션
FWSM에서 Netflow 지원
솔루션
관련 정보

소개

이 문서에서는 Cisco 6500 Series 스위치 또는 Cisco 7600 Series 라우터에 설치된 FWSM(Firewall Services Module)의 기본 컨피그레이션을 구성하는 방법에 대해 설명합니다.여기에는 원하는 트래픽을 허용하거나 원치 않는 트래픽을 차단하기 위한 IP 주소, 기본 라우팅, 고정 및 동적 NATing, ACL(Access Control Lists) 문, 내부 네트워크에서 인터넷 트래픽 검사를 위한 Websense와 같은 애플리케이션 서버, 인터넷 사용자를 위한 웹 서버의 구성이 포함됩니다.

참고: FWSM HA(High Availability) 시나리오에서 장애 조치는 모듈 간에 라이센스 키가 정확히 동일한 경우에만 성공적으로 동기화할 수 있습니다.따라서 라이센스가 다른 FWSM 간에는 장애 조치가 작동하지 않습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 3.1 이상을 실행하는 Firewall Services Module
- Catalyst 6500 Series 스위치, 필요한 구성 요소 표시:수퍼바이저 Cisco IOS 또는 Catalyst 운영 체제(OS)로 알려진 Cisco IOS® 소프트웨어를 사용하는 수퍼바이저 엔진 지원되는 수퍼바이저 엔진 및 소프트웨어 릴리스는 표를 참조하십시오.Cisco IOS 소프트웨어가 포함된 MSFC(Multilayer Switch Feature Card) 2.지원되는 Cisco IOS 소프트웨어 릴리스는 표를 참조하십시오.

[1] FWSM은 수퍼바이저 1 또는 1A를 지원하지 않습니다.

[2] 수퍼바이저에서 Catalyst OS를 사용할 경우 MSFC에서 지원되는 이러한 Cisco IOS 소프트웨어 릴리스를 사용할 수 있습니다.수퍼바이저에서 Cisco IOS 소프트웨어를 사용하는 경우 MSFC에서 동일한 릴리스를 사용합니다.

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 Cisco 7600 Series 라우터에 사용할 수 있으며, 다음과 같이 필요한 구성 요소를 사용할 수 있습니다.

- Cisco IOS 소프트웨어가 포함된 수퍼바이저 엔진지원되는 수퍼바이저 엔진 및 Cisco IOS 소프트웨어 릴리스는 표를 참조하십시오.
- MSFC 2와 Cisco IOS 소프트웨어.지원되는 Cisco IOS 소프트웨어 릴리스는 표를 참조하십시오.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

FWSM은 Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터에 설치되는 고성능 공간 절약형 스테이트풀 방화벽 모듈입니다.

방화벽은 외부 네트워크에 있는 사용자의 무단 액세스로부터 내부 네트워크를 보호합니다.또한 사용자 네트워크와 인적 자원 네트워크를 별도로 유지할 경우 방화벽은 내부 네트워크를 서로 보호할 수 있습니다.웹 또는 FTP 서버와 같이 외부 사용자가 사용할 수 있어야 하는 네트워크 리소스가 있는 경우 이러한 리소스를 방화벽 뒤에 있는 DMZ(demilitarized zone)라는 별도의 네트워크에 배치할 수 있습니다. 방화벽은 DMZ에 대한 제한된 액세스를 허용하지만, DMZ에는 공용 서버만 포함되므로, DMZ에 대한 공격은 서버에만 영향을 주며 다른 내부 네트워크에는 영향을 주지 않습니다.또한 내부 사용자가 외부 네트워크에 액세스하는 경우(예: 인터넷 액세스), 특정 주소만 외부로 허용하거나 인증 또는 권한 부여를 요구하거나 외부 URL 필터링 서버와 조정할 수 있습니다.

FWSM에는 가상화된 방화벽과 유사한 다중 보안 컨텍스트, 투명(레이어 2) 방화벽 또는 라우팅된 (레이어 3) 방화벽 운영, 수백 개의 인터페이스, 기타 다양한 기능이 포함되어 있습니다.

방화벽에 연결된 네트워크에 대한 토론 중에 외부 네트워크는 방화벽 앞에 있고 내부 네트워크는 방화벽 뒤에 보호되며 DMZ는 방화벽 뒤에 있지만 외부 사용자에게는 제한된 액세스를 허용합니다 .FWSM을 사용하면 다양한 보안 정책으로 여러 인터페이스를 구성할 수 있으므로, 여기에는 많은 내부 인터페이스, 많은 DMZ 및 필요한 경우 많은 외부 인터페이스가 포함되므로 이러한 용어는 일반적인 의미에서만 사용됩니다.

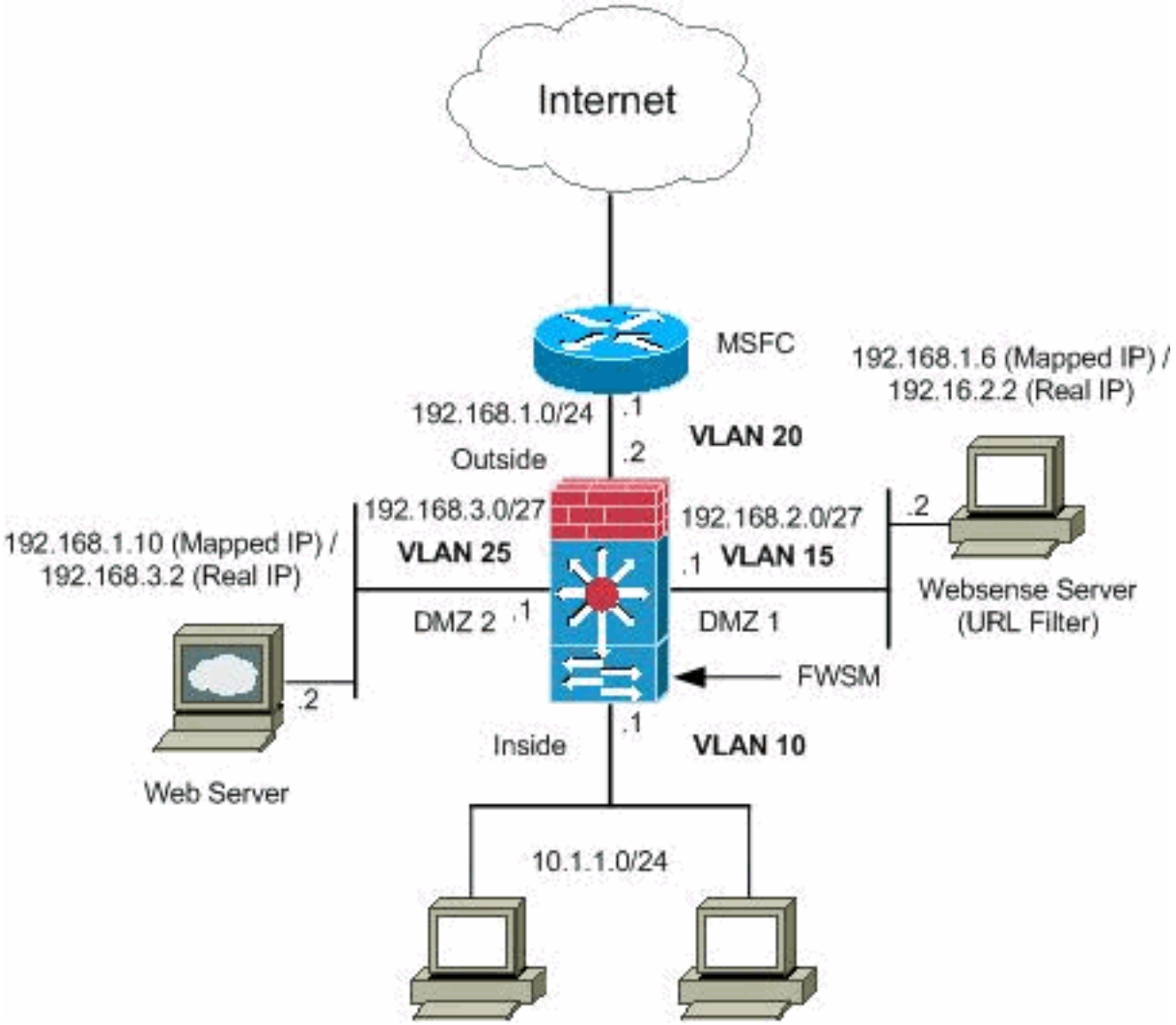
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

구성

이 문서에서는 다음 구성을 사용합니다.

- Catalyst 6500 Series 스위치 구성
- FWSM 컨피그레이션

Catalyst 6500 Series 스위치 구성

1. Catalyst 6500 Series 스위치 또는 Cisco 7600 Series 라우터에 FWSM을 설치할 수 있습니다.두 시리즈의 컨피그레이션은 동일하며 이 문서에서는 일반적으로 **스위치**로 이 시리즈를 **참조합니다.참고:** FWSM을 구성하기 전에 스위치를 적절하게 구성해야 합니다.
2. **Assign VLANs to the Firewall Services Module(방화벽 서비스 모듈에 VLAN 할당)** - 이 섹션에서는 FWSM에 VLAN을 할당하는 방법을 설명합니다.FWSM에는 외부 물리적 인터페이스가 포함되지 않습니다.대신 VLAN 인터페이스를 사용합니다.FWSM에 VLAN을 할당하는 방법은 스위치 포트에 VLAN을 할당하는 방법과 유사합니다.FWSM에는 스위치 패브릭 모듈에 대한 내부 인터페이스(있는 경우) 또는 공유 버스가 포함됩니다.**참고:** VLAN을 생성하고 스위치 포트에 할당하는 방법에 대한 자세한 내용은 Catalyst 6500 스위치 소프트웨어 구성 설명서의 VLAN 구성 섹션을 참조하십시오.**VLAN 지침:**FWSM에서 프라이빗 VLAN을 사용할 수 있습니다.FWSM에 기본 VLAN을 할당합니다.에서는 보조 VLAN 트래픽을 자동으로 처리합니다.예약된 VLAN은 사용할 수 없습니다.VLAN 1은 사용할 수 없습니다.동일한 스위치 섀시 내에서 FWSM 장애 조치를 사용하는 경우 장애 조치 및 상태 저장 통신을 위해 예약한 VLAN을 스위치 포트에 할당하지 마십시오.그러나 섀시 간 장애 조치를 사용하는 경우 섀시 간 트렁크 포트에 VLAN을 포함해야 합니다.VLAN을 FWSM에 할당하기 전에 스위치에 추가하지 않으면 VLAN은 수퍼바이저 엔진 데이터베이스에 저장되고 스위치에 추가되자마자 FWSM으로 전송됩니다.VLAN을 MSFC에 할당하기 전에 FWSM에 할당합니다.이 조건을 충족하지 않는 VLAN은 FWSM에서 할당하려고 시도하는 VLAN 범위에서 삭제됩니다.**Cisco IOS Software에서 FWSM에 VLAN을 할당합니다.**Cisco IOS 소프트웨어에서 최대 16개의 방화벽 VLAN 그룹을 생성한 다음 그룹을 FWSM에 할당합니다.예를 들어, 모든 VLAN을 하나의 그룹에 할당하거나, 내부 그룹과 외부 그룹을 생성하거나, 각 고객에 대해 그룹을 생성할 수 있습니다.각 그룹은 무제한 VLAN을 포함할 수 있습니다.동일한 VLAN을 여러 방화벽 그룹에 할당할 수 없습니다.그러나 FWSM에 여러 방화벽 그룹을 할당할 수 있으며 여러 FWSM에 단일 방화벽 그룹을 할당할 수 있습니다.예를 들어 여러 FWSM에 할당하려는 VLAN은 각 FWSM에 고유한 VLAN과 별도의 그룹에 상주할 수 있습니다.FWSM에 VLAN을 할당하려면 다음 단계를 완료합니다.

   ```
   Router(config)#firewall vlan-group firewall_group vlan_range
   ```

   vlan_range 하나 이상의 VLAN일 수 있습니다(예: 2~1000, 1025~4094). 5, 10, 15 같은 단일 숫자(n) 또는 5-10, 10-20과 같은 범위(n-x)로 식별됩니다.**참고:** 라우팅된 포트와 WAN 포트는 내부 VLAN을 사용하므로 1020-1100 범위의 VLAN이 이미 사용 중일 수 있습니다.**예:**

   ```
   firewall vlan-group 1 10,15,20,25
   ```

   방화벽 그룹을 FWSM에 할당하려면 단계를 완료합니다.

   ```
   Router(config)#firewall module module_number vlan-group firewall_group
   ```

   firewall_group은 5와 같은 단일 숫자(n) 또는 5-10과 같은 범위의 하나 이상의 그룹 번호입니다.**예:**

```
firewall module 1 vlan-group 1
```

Catalyst 운영 체제 소프트웨어의 FWSM에 VLAN 할당—Catalyst OS 소프트웨어에서 VLAN 목록을 FWSM에 할당합니다.원하는 경우 여러 FWSM에 동일한 VLAN을 할당할 수 있습니다.목록에는 무제한 VLAN이 포함될 수 있습니다.FWSM에 VLAN을 할당하려면 단계를 완료합니다.

```
Console> (enable)set vlan vlan_list firewall-vlan mod_num
```

vlan_list 하나 이상의 VLAN일 수 있습니다(예: 2~1000, 1025~4094). 5, 10, 15 같은 단일 숫자(n) 또는 5-10, 10-20과 같은 범위(n-x)로 식별됩니다.

3. **Add Switched Virtual Interfaces to the MSFC(MSFC에 스위치드 가상 인터페이스 추가)** - MSFC에 정의된 VLAN을 스위치드 가상 인터페이스라고 합니다.SVI에 사용된 VLAN을 FWSM에 할당하면 MSFC는 FWSM과 기타 레이어 3 VLAN 간에 라우팅됩니다.보안상의 이유로, 기본적으로 MSFC와 FWSM 간에는 하나의 SVI만 존재할 수 있습니다.예를 들어, 여러 SVI로 시스템을 잘못 구성하면 내부 및 외부 VLAN을 모두 MSFC에 할당하면 실수로 트래픽이 FWSM을 통과하도록 허용할 수 있습니다.SVI를 구성하려면 단계를 완료합니다.

```
Router(config)#interface vlan vlan_number
Router(config-if)#ip address address mask
```

예:

```
interface vlan 20
ip address 192.168.1.1 255.255.255.0
```

Catalyst 6500 Series 스위치 구성
`!--- Output Suppressed` firewall vlan-group 1 10,15,20,25 firewall module 1 vlan-group 1 interface vlan 20 ip address 192.168.1.1 255.255.255.0 `!--- Output Suppressed`

참고: 스위치 운영 체제에 적합한 명령을 사용하여 스위치에서 FWSM에 대한 세션을 시작합니다.

- Cisco IOS 소프트웨어:

```
Router#session slot
```

- Catalyst OS 소프트웨어:

```
Console> (enable) session module_number
```

(선택 사항) 다른 서비스 모듈과 VLAN 공유 - 스위치에 다른 서비스 모듈(예: ACE)이 있는 경우 일부 VLAN을 이러한 서비스 모듈과 공유해야 할 수 있습니다.FWSM 컨피그레이션을 최적화하는 방법에 대한 자세한 내용은 ACE 및 FWSM을 사용한 서비스 모듈 설계를 참조하십시오.

FWSM 컨피그레이션

1. **Configure Interfaces for FWSM**(FWSM용 인터페이스 구성) - FWSM을 통한 트래픽을 허용하

려면 먼저 인터페이스 이름 및 IP 주소를 구성해야 합니다.또한 보안 레벨을 기본값인 0에서 변경해야 합니다. 인터페이스의 이름을 지정하고 보안 레벨을 명시적으로 설정하지 않으면 FWSM은 보안 레벨을 100으로 설정합니다.**참고:** 각 인터페이스에는 0(최저)에서 100(최고)까지의 보안 레벨이 있어야 합니다. 예를 들어, 내부 호스트 네트워크와 같이 가장 안전한 네트워크를 레벨 100에 할당해야 하며 인터넷에 연결된 외부 네트워크는 레벨 0이 될 수 있습니다. DMZ와 같은 다른 네트워크는 그 사이에 있을 수 있습니다.컨피그레이션에 VLAN ID를 추가할 수 있지만, 스위치에서 FWSM에 할당한 10, 15, 20 및 25와 같은 VLAN만 트래픽을 전달할 수 있습니다.FWSM에 할당된 모든 VLAN을 보려면 **show vlan** 명령을 사용합니다.

```
interface vlan 20
    nameif outside
    security-level 0
    ip address 192.168.1.2 255.255.255.0
interface vlan 10
    nameif inside
    security-level 100
    ip address 10.1.1.1 255.255.255.0
interface vlan 15
    nameif dmz1
    security-level 60
    ip address 192.168.2.1 255.255.255.224
interface vlan 25
    nameif dmz2
    security-level 50
    ip address 192.168.3.1 255.255.255.224
```

팁: nameif *<name> 명령*에서 *이름*은 최대 48자의 텍스트 문자열이며 대/소문자를 구분하지 않습니다.새 값으로 이 명령을 다시 입력할 경우 이름을 변경할 수 있습니다.no 형식을 입력하지 마십시오. 이 명령은 해당 이름을 참조하는 모든 명령을 삭제합니다.

2. **기본 경로를 구성합니다.**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

기본 경로는 FWSM이 학습 또는 고정 경로가 없는 모든 IP 패킷을 전송하는 게이트웨이 IP 주소(192.168.1.1)을 식별합니다.기본 경로는 단순히 목적지 IP 주소로 0.0.0.0/0을 사용하는 고정 경로입니다.특정 대상을 식별하는 경로가 기본 경로보다 우선합니다.

3. **동적 NAT**는 실제 주소 그룹(10.1.1.0/24)을 대상 네트워크에서 라우팅 가능한 매핑된 주소 풀(192.168.1.20-192.168.1.50)으로 변환합니다.매핑된 풀은 실제 그룹보다 더 적은 수의 주소를 포함할 수 있습니다.변환하려는 호스트가 대상 네트워크에 액세스하면 FWSM은 매핑된 풀의 IP 주소를 할당합니다.실제 호스트가 연결을 시작할 때만 변환이 추가됩니다.변환은 연결 기간 동안에만 수행되며, 변환 시간이 초과된 후에는 지정된 사용자가 동일한 IP 주소를 유지하지 않습니다.

```
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 192.168.1.20-192.168.1.50 netmask 255.255.255.0
access-list Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any
access-group Internet in interface inside
```

내부 네트워크 10.1.1.0/24에서 DMZ1 네트워크(192.168.2.0)으로 이동하는 트래픽을 거부하고 ACL *인터넷*을 내부 인터페이스에 내부 트래픽의 방향으로 적용하여 인터넷에 대한 다른 종류의 트래픽을 허용하려면 ACL을 생성해야 합니다.

4. **고정 NAT**는 실제 주소의 고정 변환을 매핑된 주소로 생성합니다.동적 NAT 및 PAT를 사용하면 각 호스트는 후속 변환마다 다른 주소 또는 포트를 사용합니다.매핑된 주소는 고정 NAT와

의 각 연속 연결에 대해 동일하며 영구 변환 규칙이 존재하기 때문에, 고정 NAT는 대상 네트워크의 호스트가 변환된 호스트에 대한 트래픽을 시작할 수 있도록 허용합니다(액세스 목록이 있는 경우).동적 NAT와 고정 NAT의 주소 범위 간의 주요 차이점은 고정 NAT는 원격 호스트가 변환된 호스트에 대한 연결을 시작할 수 있도록 허용하지만, 이를 허용하는 액세스 목록이 있는 경우 동적 NAT는 이를 허용하지 않는다는 것입니다.또한 고정 NAT를 사용하는 실제 주소로 동일한 수의 매핑된 주소가 필요합니다.

```
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255
access-list outside extended permit tcp any host 192.168.1.10 eq http
access-list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-
data
access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-
status
access-list inbound extended permit udp any host 216.70.55.69 range 8766 30000
access-group outside in interface outside
```

다음은 표시된 두 개의 고정 NAT 문입니다.첫 번째 방법은 내부 인터페이스의 실제 IP 192.168.2.2을 외부 서브넷의 매핑된 IP 192.168.1.6으로 변환하는 것입니다. 단, DMZ1 네트워크의 Websense 서버에 액세스하기 위해 소스 192.168.1.30에서 매핑된 IP 192.168.1.6으로 트래픽을 허용할 수 있습니다.마찬가지로, 내부 인터페이스의 실제 IP 192.168.3.2을 외부 서브넷의 매핑된 IP 192.168.1.10으로 변환하는 두 번째 정적 NAT 문은 DMZ2 네트워크의 웹 서버에 액세스하고 8766~30000 범위의 udp 포트 번호를 가질 수 있도록 ACL이 인터넷에서 매핑된 IP 192.168.1.10으로 트래픽을 허용하는 경우에 제공됩니다.

5. url-server 명령은 Websense URL 필터링 애플리케이션을 실행하는 서버를 지정합니다.한계는 단일 컨텍스트 모드의 URL 서버 16개와 다중 모드의 URL 서버 4개입니다. 그러나 한 번에 하나의 애플리케이션(N2H2 또는 Websense)만 사용할 수 있습니다.또한 보안 어플라이언스에서 컨피그레이션을 변경할 경우 애플리케이션 서버의 컨피그레이션이 업데이트되지 않습니다.이 작업은 공급업체의 지침에 따라 별도로 수행해야 합니다.HTTPS 및 FTP에 대해 filter 명령을 실행하려면 먼저 url-server 명령을 구성해야 합니다.모든 URL 서버가 서버 목록에서 제거되면 URL 필터링과 관련된 모든 필터 명령도 제거됩니다.서버를 지정한 후 filter url 명령을 사용하여 URL 필터링 서비스를 활성화합니다.

```
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1
connections 5
```

filter url 명령을 사용하면 Websense 필터링 애플리케이션으로 지정한 World Wide Web URL에서 아웃바운드 사용자에 대한 액세스를 방지할 수 있습니다.

```
filter url http 10.1.1.0 255.255.255.0 0 0
```

FWSM 컨피그레이션
!--- Output Suppressed interface vlan 20 nameif outside security-level 0 ip address 192.168.1.2 255.255.255.0 interface vlan 10 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0 interface vlan 15 nameif dmz1 security-level 60 ip address 192.168.2.1 255.255.255.224 interface vlan 25 nameif dmz2 security- level 50 ip address 192.168.3.1 255.255.255.224 passwd fl0wer enable password treeh0u$e route outside 0 0

```
192.168.1.1 1 url-server (dmz1) vendor websense host
192.168.2.2 timeout 30 protocol TCP version 1
connections 5 url-cache dst 128 filter url http 10.1.1.0
255.255.255.0 0 0 !--- When inside users access an HTTP
server, FWSM consults with a !--- Websense server in
order to determine if the traffic is allowed. nat
(inside) 1 10.1.1.0 255.255.255.0 global (outside) 1
192.168.1.20-192.168.1.50 netmask 255.255.255.0 !---
Dynamic NAT for inside users that access the Internet
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask
255.255.255.255 !--- A host on the subnet 192.168.1.0/24
requires access to the Websense !--- server for
management that use pcAnywhere, so the Websense server
!--- uses a static translation for its private address.
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask
255.255.255.255 !--- A host on the Internet requires
access to the Webserver, so the Webserver !--- uses a
static translation for its private address. access-list
Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any access-
group Internet in interface inside !--- Allows all
inside hosts to access the outside for any IP traffic,
!--- but denies them access to the dmz1 access-list
outside extended permit tcp any host 192.168.1.10 eq
http !--- Allows the traffic from the internet with the
destination IP address !--- 192.168.1.10 and destination
port 80 access-list outside extended permit tcp host
192.168.1.30 host 192.168.1.6 eq pcanywhere-data access-
list outside extended permit udp host 192.168.1.30 host
192.168.1.6 eq pcanywhere-status !--- Allows the
management host 192.168.1.30 to use !--- pcAnywhere on
the Websense server access-list inbound extended permit
udp any host 216.70.55.69 range 8766 30000 !--- Allows
udp port number in the range of 8766 to 30000. access-
group outside in interface outside access-list WEBSENSE
extended permit tcp host 192.168.2.2 any eq http access-
group WEBSENSE in interface dmz1 !--- The Websense
server needs to access the Websense !--- updater server
on the outside. !--- Output Suppressed
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

1. 스위치가 FWSM을 승인하고 온라인으로 전환했는지 확인하려면 운영 체제에 따라 모듈 정보를 확인하십시오.Cisco IOS 소프트웨어:

```
Router#show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1     2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD0444099Y
  2    48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03475619
  3     2  Intrusion Detection System             WS-X6381-IDS       SAD04250KV5
  4     6  Firewall Module                        WS-SVC-FWM-1       SAD062302U4
```

Catalyst OS 소프트웨어:

```
Console>show module [mod-num]
```

```
The following is sample output from the show module command:

Console> show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- ------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
4   4    2     Intrusion Detection Syste WS-X6381-IDS        no  ok
5   5    6     Firewall Module           WS-SVC-FWM-1        no  ok
6   6    8     1000BaseX Ethernet        WS-X6408-GBIC       no  ok
```

참고: show **module** 명령은 FWSM에 대한 6개의 포트를 표시합니다.이는 EtherChannel로 그룹화된 내부 포트입니다.

2.
```
Router#show firewall vlan-group
Group vlans
----- ------
   1 10,15,20
   51 70-85
   52 100
```

3.
```
Router#show firewall module
Module Vlan-groups
  5    1,51
  8    1,52
```

4. 현재 부트 파티션을 보려면 운영 체제에 대한 명령을 입력합니다.Cisco IOS 소프트웨어:
```
Router#show boot device [mod_num]
```

예:
```
Router#show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

Catalyst OS 소프트웨어:
```
Console> (enable) show boot device mod_num
```

예:
```
Console> (enable) show boot device 6
Device BOOT variable = cf:5
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

1. **Setting the Default Boot Partition(기본 부팅 파티션 설정)** - 기본적으로 FWSM은 cf:**4** 애플리케이션 파티션에서 부팅됩니다.그러나 cf:**5** 애플리케이션 파티션 또는 **cf:1** 유지 관리 파티션으로 부팅하도록 선택할 수 있습니다.기본 부팅 파티션을 변경하려면 운영 체제에 대한 명령을 입력합니다.Cisco IOS 소프트웨어:
```
Router(config)#boot device module mod_num cf:n
```

여기서 n은 1(유지 보수), 4(애플리케이션) 또는 5(애플리케이션)입니다.Catalyst OS 소프트웨

어:

```
Console> (enable) set boot device cf:n mod_num
```

여기서 n은 1(유지 보수), 4(애플리케이션) 또는 5(애플리케이션)입니다.

2. **Cisco IOS Software에서 FWSM 재설정** - FWSM을 재설정하려면 다음과 같이 명령을 입력합니다.

```
Router#hw-module module mod_num reset [cf:n] [mem-test-full]
```

cf:n 인수는 1(유지 관리), 4(애플리케이션) 또는 5(애플리케이션)의 파티션입니다. 파티션을 지정하지 않으면 기본 파티션이 사용됩니다. 일반적으로 **cf:4**.mem-**test-full** 옵션은 전체 메모리 테스트를 실행하며, 이 테스트는 약 6분이 소요됩니다.**예:**

```
Router#hw-mod module 9 reset
Proceed with reload of module? [confirm] y
% reset issued for module 9
Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

Catalyst **OS** 소프트웨어:

```
Console> (enable) reset mod_num [cf:n]
```

여기서 **cf:n**은 1(유지 보수), 4(애플리케이션) 또는 5(애플리케이션) 파티션입니다. 파티션을 지정하지 않으면 기본 파티션이 사용됩니다. 일반적으로 **cf:4**.

참고: NTP는 스위치에서 설정을 사용하므로 FWSM에서 구성할 수 없습니다.

문제/장애:FWSM에서 IPS 센서 4270으로 VLAN 트래픽을 전달할 수 없습니다.

FWSM에서 IPS 센서로 트래픽을 전달할 수 없습니다.

솔루션

IPS를 통해 트래픽을 강제로 전달하려면 현재 VLAN 중 하나를 효과적으로 두 개로 분할한 다음 서로 연결하기 위해 보조 VLAN을 생성하는 것이 요령입니다.VLAN 401 및 501에서 이 예를 확인하여 다음을 명확히 하십시오.

- 기본 VLAN **401**에서 트래픽을 스캔하려면 다른 vlan **VLAN 501**(보조 VLAN)을 생성합니다. 그런 다음 401의 호스트가 현재 기본 게이트웨이로 사용하는 VLAN 인터페이스 401을 비활성화합니다.
- 그런 다음 VLAN 401 인터페이스에서 이전에 비활성화했던 *동일한* 주소로 VLAN 501 인터페이스를 활성화합니다.
- VLAN 401에는 IPS 인터페이스 중 하나를, VLAN 501에는 다른 인터페이스를 배치합니다.

VLAN 401의 기본 게이트웨이를 VLAN 501로 이동하기만 하면 됩니다. VLAN이 있는 경우 유사한 변경을 수행해야 합니다.VLAN은 기본적으로 LAN 세그먼트와 유사합니다.기본 게이트웨이를 사용하는 호스트와 다른 와이어에 사용할 수 있습니다.

FWSM에서 Out-Of-Order 패킷 문제

FWSM에서 Out-of-Order 패킷 문제를 해결하려면 어떻게 해야 합니까?

솔루션

FWSM에서 Out-Of-Order 패킷 문제를 해결하려면 전역 컨피그레이션 모드에서 sysopt np completion-unit 명령을 실행합니다.이 명령은 FWSM 버전 3.2(5)에 도입되었으며 패킷이 수신한 것과 동일한 순서로 전달되도록 합니다.

문제/장애:비대칭 라우팅 패킷을 방화벽을 통해 전달할 수 없습니다.

비대칭 라우팅 패킷을 방화벽을 통해 전달할 수 없습니다.

솔루션

비대칭 라우팅 패킷을 방화벽을 **통해 전달하려면 클래스 컨피그레이션** 모드에서 set connection advanced-options tcp-state-bypass 명령을 실행합니다.이 명령은 FWSM 버전 3.2(1)에 도입되었습니다.

FWSM에서 Netflow 지원

FWSM은 Netflow를 지원합니까?

솔루션

Netflow는 FWSM에서 지원되지 않습니다.

관련 정보

- Cisco Catalyst 6500 Series 방화벽 서비스 모듈 지원 페이지
- Cisco Catalyst 6500 Series 스위치 지원 페이지
- Cisco 7600 Series 라우터 지원 페이지
- FWSM TCP 인터셉트 및 SYN 쿠키가 설명
- 기술 지원 및 문서 – Cisco Systems