Voorbeeld van configuratie van FWSM

Inhoud

Inleiding

Dit document beschrijft hoe u de basisconfiguratie van de Firewallservicesmodule (FWSM) kunt configureren die in Cisco 6500 Series-switches of Cisco 7600 Series routers is geïnstalleerd. Dit omvat de configuratie van het IP-adres, de standaardrouting, statische en dynamische NATing, toegangscontrolelijsten (ACL's) om het gewenste verkeer toe te staan of het ongewenste verkeer te blokkeren, toepassingsservers zoals Webason voor de inspectie van het internetverkeer vanuit het binnennetwerk en de Webserver voor internetgebruikers.

Opmerking: In een scenario met hoge beschikbaarheid van FWSM (HA) kan de failover alleen succesvol sync's zijn wanneer de licentietoetsen precies hetzelfde zijn tussen de modules. Daarom kan de failover niet tussen de FWSM's met verschillende licenties werken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firewallservicesmodule waarmee softwareversie 3.1 en hoger wordt uitgevoerd
- Catalyst 6500 Series-switches, met de vereiste onderdelen zoals aangegeven:Supervisor Engine met Cisco IOS® software, die bekend staat als supervisor Cisco IOS, of Catalyst besturingssysteem (OS). Zie Tabel voor ondersteunde Supervisor Engine en software releases.functiekaart voor meerlaagse switch (MSFC) 2 met Cisco IOS-software. Zie Tabel voor ondersteunde Cisco IOS-softwarereleases.

[1] De FWSM ondersteunt supervisor 1 of 1A niet.

[2] Wanneer u Catalyst OS op de supervisor gebruikt, kunt u een van deze ondersteunde Cisco IOS-softwarereleases op de MSFC gebruiken. Wanneer u Cisco IOS-software op de supervisor gebruikt, gebruikt u dezelfde release op de MSFC.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt voor de Cisco 7600 Series routers, met de vereiste onderdelen zoals wordt weergegeven:

- Supervisor Engine met Cisco IOS-software. Zie Tabel voor ondersteunde Supervisor Engine en Cisco IOS-softwarereleases.
- MSFC 2 met Cisco IOS-software. Zie Tabel voor ondersteunde Cisco IOS-softwarereleases.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

FWSM is een krachtige, ruimtebesparende, stateful firewallmodule die in de Catalyst 6500 Series switches en Cisco 7600 Series routers installeert.

Firewalls beschermen binnen netwerken tegen toegang door onbevoegden op een extern netwerk. De firewall kan ook binnen netwerken tegen elkaar beschermen, bijvoorbeeld, wanneer u een netwerk van menselijke middelen gescheiden houdt van een gebruikersnetwerk. Als u netwerkbronnen hebt die beschikbaar moeten zijn voor een externe gebruiker, zoals een web- of FTP-server, kunt u deze bronnen op een afzonderlijk netwerk achter de firewall plaatsen, die een gedemilitariseerde zone (DMZ) wordt genoemd. De firewall staat beperkte toegang tot de DMZ toe, maar omdat de DMZ alleen de openbare servers bevat, heeft een aanval alleen gevolgen voor de servers en heeft ze geen invloed op de andere binnennetwerken. U kunt ook controle

hebben als binnengebruikers toegang hebben tot buiten netwerken, bijvoorbeeld toegang tot het internet, als u alleen bepaalde adressen toestaat, verificatie of autorisatie vereist of coördineert met een externe URL-filterserver.

FWSM omvat vele geavanceerde functies, zoals meerdere veiligheidscontexten die vergelijkbaar zijn met gevirtualiseerde firewalls, transparante (Layer 2) firewall of routed (Layer 3) firewallwerking, honderden interfaces en veel meer functies.

Tijdens de discussie over netwerken die zijn aangesloten op een firewall, is het buitennetwerk voor de firewall, het binnennetwerk beschermd en achter de firewall, en een DMZ, terwijl achter de firewall, beperkte toegang tot externe gebruikers toestaat. Omdat FWSM u veel interfaces met gevarieerd veiligheidsbeleid laat configureren, dat veel binneninterfaces, veel DMZ's en zelfs veel buiteninterfaces omvat, indien gewenst, worden deze termen slechts in algemene zin gebruikt.

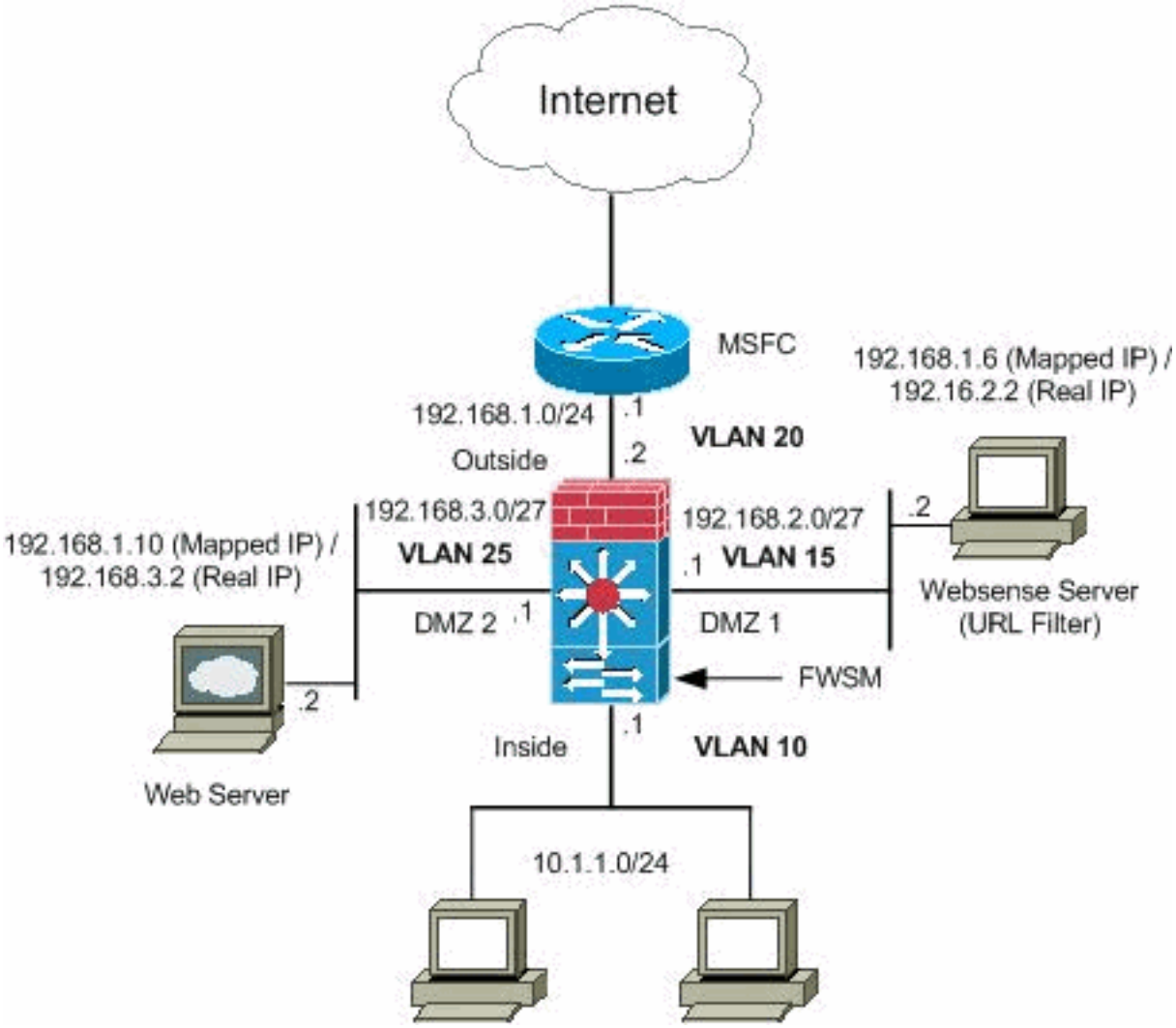
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918-adressen, die in een labomgeving zijn gebruikt.

Configuraties

Dit document gebruikt deze configuraties:

- Catalyst 6500 Series switchconfiguratie
- FWSM-configuratie

Catalyst 6500 Series switchconfiguratie

1. U kunt FWSM in Catalyst 6500 Series switches voor Cisco 7600 Series routers installeren. De configuratie van beide reeksen is identiek en de reeksen worden in dit document algemeen als de **schakelaar** vermeld.**Opmerking:** U dient de schakelaar correct te configureren voordat u FWSM configureren.
2. **Toewijzen van VLAN's aan de module van de Firewall** - Deze sectie beschrijft hoe u VLAN's aan FWSM wilt toewijzen. De FWSM bevat geen externe fysieke interfaces. In plaats daarvan gebruikt het VLAN-interfaces. Toewijzen van VLAN's aan FWSM is gelijkaardig aan hoe u een VLAN aan een switchpoort toewijst; FWSM bevat een interne interface naar de switchfabric-module, indien aanwezig, of de gedeelde bus.**N.B.:** Raadpleeg het gedeelte

VLAN's configureren van de Catalyst 6500 Switches softwareconfiguratie Guide voor meer informatie over het maken van VLAN's en het toewijzen aan switchpoorten.**VLAN-richtlijnen:**U kunt privé VLAN's met de FWSM gebruiken. het primaire VLAN aan FWSM toewijzen; FWSM behandelt automatisch secundair VLAN-verkeer.U kunt gereserveerde VLAN's niet gebruiken.U kunt VLAN 1 niet gebruiken.Als u FWSM failover binnen één zelfde switchchassis gebruikt, wijs niet de VLAN(s) toe die u gereserveerd hebt voor failover en stateful communications aan een switchpoort. Maar als u failover tussen chassis gebruikt, moet u de VLAN's in de boomkpoort tussen de chassis opnemen.Als u de VLAN's aan de switch niet toevoegt voordat u ze aan FWSM toewijst, worden de VLAN's opgeslagen in de Supervisor Engine database en naar FWSM verzonden zodra ze aan de switch worden toegevoegd.Pas VLAN's aan FWSM voordat u ze aan de MSFC toewijst.VLAN's die niet aan deze voorwaarde voldoen, worden van het bereik van VLAN's verwijderd dat u op FWSM wilt toewijzen.**Toewijzen VLAN's aan FWSM in Cisco IOS-software:**In Cisco IOS-software kunt u maximaal 16 VLAN-firewallgroepen maken en vervolgens de groepen aan FWSM toewijzen. U kunt bijvoorbeeld alle VLAN's aan één groep toewijzen of u kunt een binnengroep en een externe groep maken of u kunt een groep voor elke klant maken. Elke groep kan onbeperkte VLAN's bevatten.U kunt hetzelfde VLAN niet aan meerdere firewallgroepen toewijzen; U kunt echter meerdere firewallgroepen aan een FWSM toewijzen en u kunt één firewallgroep aan meerdere FWSM's toewijzen. VLAN's die u wilt toewijzen aan meerdere FWSM's, kunnen bijvoorbeeld in een afzonderlijke groep van VLAN's verblijven die uniek zijn voor elke FWSM.Voltooi de stappen om VLAN's aan FWSM toe te wijzen:

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

De `vlan_range` kan één of meer VLAN's zijn, bijvoorbeeld, 2 tot 1000 en van 1025 tot 4094, geïdentificeerd als één getal (n) zoals 5, 10, 15 of een bereik (n-x) zoals 5-10, 10-20.**Opmerking:** Routed poorten en WAN-poorten gebruiken interne VLAN's, zodat het mogelijk is dat VLAN's in de 1020-100-reeks al in gebruik zijn.**Voorbeeld:**

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

Voltooi de stappen om de firewallgroepen aan het FWSM te toewijzen.

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

The `firewall_group` is één of meer groepsgetallen als één enkel aantal (n) zoals 5 of een bereik als 5-10.**Voorbeeld:**

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

Toewijzen VLAN's aan FWSM in Catalyst Besturingssoftware - In Catalyst OS software, wijst u een lijst van VLANs aan FWSM toe. U kunt hetzelfde VLAN desgewenst aan meerdere FWSM's toewijzen. De lijst kan onbeperkte VLAN's bevatten.Voltooi de stappen om VLAN's aan FWSM toe te wijzen.

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

De `vlan_list` kan één of meer VLAN's zijn, bijvoorbeeld, 2 tot 1000 en van 1025 tot 4094, geïdentificeerd als één enkel aantal (n) zoals 5, 10, 15 of een bereik (n-x) zoals 5-10, 10-20.

3. **Voeg switched virtuele interfaces toe aan de MSFC**-A VLAN die op de MSFC zijn gedefinieerd, wordt een switched virtuele interface genoemd. Als u het VLAN toewijst dat voor SVI aan FWSM wordt gebruikt, dan de MSFC routes tussen FWSM en andere Layer 3

VLAN's.Om veiligheidsredenen kan standaard slechts één SVI bestaan tussen de MSFC en het FWSM. Als u het systeem bijvoorbeeld verkeerd instelt met meerdere SVI's, kunt u per ongeluk verkeer toestaan om rond de FWSM door te geven als u zowel de binnen- als buitenkant VLAN's aan de MSFC toewijst.Volg de stappen om de SVI te configureren

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

Voorbeeld:

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

Catalyst 6500 Series switchconfiguratie
`!--- 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`

Opmerking: Sessie in naar FWSM vanaf de schakelaar met de opdracht geschikt voor uw schakelaar besturingssysteem:

- Cisco IOS-software:
  ```
  Router#session slot
  ```

- Catalyst IOS-software:
  ```
  Console> (enable) session module_number
  ```

(Optioneel) VLAN's delen met andere servicemodules - Als de switch andere servicemodules heeft, bijvoorbeeld Application Control Engine (ACE), is het mogelijk dat u bepaalde VLAN's met deze servicemodules moet delen. Raadpleeg het gedeelte Servicemodule Design met ACE en FWSM voor meer informatie over het optimaliseren van de FWSM-configuratie wanneer u met dergelijke andere modules werkt.

FWSM-configuratie

1. **Configureer interfaces voor FWSM** - Voordat u verkeer door de FWSM kunt toestaan, moet u een interfacenaam en een IP-adres configureren. U dient het beveiligingsniveau ook te wijzigen van de standaardinstelling, die 0 is. Als u een interface `binnenin` noemt en u het beveiligingsniveau niet expliciet instelt, stelt FWSM het beveiligingsniveau in op 100.**Opmerking:** elke interface moet een beveiligingsniveau hebben van 0 (laagste) tot 100 (hoogste). Bijvoorbeeld, zou u uw best veilige netwerk, zoals het binnennetwerk van de gastheer, aan niveau 100 moeten toewijzen, terwijl het buitennetwerk dat op Internet wordt aangesloten niveau 0 kan zijn. Andere netwerken, zoals DMZs, kunnen tussenin zijn.U kunt elke VLAN-id aan de configuratie toevoegen, maar alleen VLAN's, bijvoorbeeld 10, 15, 20 en 25, die door de switch aan FWSM worden toegewezen, kunnen verkeer doorgeven. Gebruik

de opdracht **show VLAN** om alle VLAN's te bekijken die aan FWSM zijn toegewezen.

```
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
```

Tip: Onder **de** naam**, als** ***<naam>***, *is* de *naam* een tekststring die maximaal 48 tekens bevat en die niet hoofdlettergevoelig is. U kunt de naam wijzigen als u deze opdracht opnieuw met een nieuwe waarde invoert. Typ het no-formulier niet, omdat deze opdracht ervoor zorgt dat alle opdrachten die naar deze naam verwijzen, worden verwijderd.

2. **Configureer de standaardroute:**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

Een standaardroute identificeert het IP-adres van de gateway (192.168.1.1) waarnaar FWSM alle IP-pakketten verstuurt waarvoor het geen geleerde of statische route heeft. Een standaardroute is eenvoudig een statische route met 0.0.0.0/0 als het bestemming IP-adres. Routes die een specifieke bestemming identificeren hebben voorrang boven de standaardroute.

3. **Dynamische NAT** vertaalt een groep echte adressen (10.1.1.0/24) naar een pool van in kaart gebrachte adressen (192.168.1.20-192.168.1.50) die op het doelnetwerk routeerbaar zijn. De in kaart gebrachte pool kan minder adressen bevatten dan de echte groep. Wanneer een host die u wilt vertalen, toegang tot het doelnetwerk krijgt, wijst FWSM het een IP-adres uit de in kaart gebrachte pool toe. De vertaling wordt slechts toegevoegd wanneer de echte host de verbinding start. De vertaling is alleen beschikbaar voor de duur van de verbinding, en een bepaalde gebruiker behoudt na de vertaaltijden niet hetzelfde IP-adres.

```
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
```

U moet een ACL creëren om het verkeer van het binnennetwerk 10.1.1.0/24 te ontkennen om naar het netwerk DMZ1 te gaan (192.168.2.0) en andere soorten verkeer naar het internet toe te staan door toepassing van het ACL *Internet* op de binneninterface als binnenrichting voor inkomend verkeer.

4. **Static NAT** maakt een vaste vertaling van het (de) echte adres(sen) naar het (de) in kaart gebrachte adres(sen).Met Dynamic NAT en PAT gebruikt elke host een ander adres of poort voor elke volgende vertaling. Omdat het in kaart gebrachte adres hetzelfde is voor elke opeenvolgende verbinding met statische NAT en er een persistente vertaalregel bestaat,

staat statische NAT hosts op het doelnetwerk toe om verkeer naar een vertaalde host te openen, als er een toegangslijst is die dit toestaat.Het belangrijkste verschil tussen dynamische NAT en een reeks adressen voor statische NAT is dat statische NAT een afstandsbediening toestaat om een verbinding naar een vertaalde host te openen als er een toegangslijst is die dit toestaat, terwijl dynamisch NAT niet. U hebt ook een gelijk aantal in kaart gebrachte adressen nodig als echte adressen met statische NAT.

```
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
```

Dit zijn de twee statische NAT-verklaringen die worden getoond. Het eerste moet de echte IP 192.168.2.2 op de interne interface naar het in kaart gebrachte IP 192.168.1.6 op het buitennet vertalen, op voorwaarde dat ACL het verkeer vanaf bron 192.168.1.30 naar de in kaart gebrachte IP 192.168.1 toestaat 6 om toegang te krijgen tot de weblogserver in het DMZ1-netwerk. Op dezelfde manier is de tweede statische NAT-verklaring die bedoeld is om de echte IP 192.168.3.2 op de binneninterface te vertalen naar de in kaart gebrachte IP 192.168.1.10 op het buitennet, op voorwaarde dat ACL het verkeer van het internet naar de in kaart gebrachte IP 192.168.1.10 toestaat om toegang tot de Webserver in het DMZ2-netwerk en hebben het udp-poortnummer tussen 8766 en 30000.

5. De opdracht **url-server** wijst de server aan die de Websin URL-filtertoepassing aanvoert. De limiet is 16 URL-servers in één contextmodus en vier URL-servers in multi-mode, maar u kunt slechts één toepassing tegelijkertijd gebruiken, of N2H2 of Websing. Als u bovendien uw configuratie op het beveiligingsapparaat wijzigt, wordt de configuratie op de toepassingsserver niet bijgewerkt. Dit moet afzonderlijk gebeuren, overeenkomstig de verkoopinstructies.De opdracht **url-server** moet worden geconfigureerd voordat u de filteropdracht voor HTTPS en FTP geeft. Als alle URL-servers van de serverlijst worden verwijderd, worden alle filteropdrachten met betrekking tot URL-filtering ook verwijderd.Nadat u de server hebt aangewezen, stelt u de URL-filterservice in met de opdracht **filter**.

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

De opdracht **filter url** staat de preventie van toegang van uitgaande gebruikers van het World Wide Web URLS toe die u aanwijst met de toepassing WebSensfilter.

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

FWSM-configuratie
!--- 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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

1. Bekijk de module informatie in overeenstemming met uw besturingssysteem om te controleren of de switch de FWSM erkent en deze online heeft gebracht:Cisco IOS-software:

```
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 IOS-software:

```
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
```

Opmerking: de opdracht **Show module** toont zes poorten voor FWSM. Dit zijn interne poorten die gegroepeerd zijn als EtherChannel.

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. Geef de opdracht voor het besturingssysteem op om de huidige opstart-indeling te bekijken:Cisco IOS-software:

```
Router#show boot device [mod_num]
```

Voorbeeld:

```
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 IOS-software:

```
Console> (enable) show boot device mod_num
```

Voorbeeld:

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

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

1. **De standaardinstelling van de opstartverdeling** - Standaard **start** de FWSM-laars vanaf de **cf:4** toepassingsverdeling. Maar u kunt ervoor kiezen om te beginnen vanaf de **cf:5** applicatie

of in de **cf:1** onderhoudspartitie. Voer de opdracht voor het besturingssysteem in om de standaardopstartverdeling te wijzigen:Cisco IOS-software:

```
Router(config)#boot device module mod_num cf:n
```

Indien n 1 (onderhoud), 4 (toepassing) of 5 (toepassing) is.Catalyst IOS-software:

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

Indien n 1 (onderhoud), 4 (toepassing) of 5 (toepassing) is.

2. **Het terugstellen van FWSM in Cisco IOS software**-Om het FWSM opnieuw in te stellen, voer de opdracht in zoals getoond:

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

Het **cf:n** argument is de verdeling, ofwel 1 (onderhoud), 4 (toepassing), ofwel 5 (toepassing). Als u de partitie niet specificeert, wordt de standaardpartitie gebruikt, die normaal **cf:4** is.De **mem-test-Full** optie voert een volledige geheugentest uit, die ongeveer zes minuten in beslag neemt.**Voorbeeld:**

```
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 ...
```

Voor **Catalyst OS**-software:

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

Indien **cf:n** de verdeling is, hetzij 1 (onderhoud), 4 (toepassing), hetzij 5 (toepassing). Als u de partitie niet specificeert, wordt de standaardpartitie gebruikt, die normaal **cf:4** is.

Opmerking: NTP kan niet worden ingesteld op FWSM, omdat het zijn instellingen uit de switch haalt.

Probleem: Kan het VLAN-verkeer niet van FWSM naar de IPS-sensor (4270)

U kunt het verkeer niet van FWSM naar de IPS sensoren doorgeven.

Oplossing

Om verkeer door IPS te dwingen, is de truc om een hulpVLAN te creëren om één van uw huidige VLAN's in twee effectief te breken en hen dan samen te overbruggen. Controleer dit voorbeeld met VLAN 401 en 501 om meer duidelijkheid te geven:

- Als u verkeer op belangrijkste **VLAN 401** wilt scannen, kunt u een ander VLAN **VLAN 501** (auxillary VLAN) maken. Toen schakelt u de VLAN-interface 401 uit, die de hosts in 401 momenteel gebruiken als hun standaardgateway.
- Stel vervolgens VLAN 501-interface in met *hetzelfde* adres dat u eerder op de VLAN 401-interface hebt uitgeschakeld.
- Plaats een van de IPS-interfaces in VLAN 401 en de andere in VLAN 501.

U hoeft de standaardgateway voor VLAN 401 alleen maar naar VLAN 501 te verplaatsen. U moet de soortgelijke wijzigingen voor VLAN’s doen indien aanwezig. Merk op dat VLAN’s in wezen net als LAN-segmenten zijn. U kunt een standaardgateway hebben op een ander draadstuk dan de hosts die het gebruiken.

Out-order pakketten uitgegeven in FWSM

Hoe kan ik het probleem van de out-of-order pakketjes in FWSM oplossen?

Oplossing

Geef het systeem np-voltooiing-unit **comand uit in de mondiale configuratiemodus om de out-of-order pakketprobleem in FWSM op te lossen.** Deze opdracht is geïntroduceerd in FWSM versie 3.2(5) en zorgt ervoor dat pakketten worden verzonden in de dezelfde volgorde als ze werden ontvangen.

Probleem: Kan asymmetrisch routed pakketten niet door de firewall doorgeven

U kunt niet asymmetrisch routed pakketten door de firewall laten passeren.

Oplossing

Geef de ingestelde opdracht voor geavanceerde-optieopties op TCP-state-bypass in de klasse-configuratiemodus om asymmetrisch routed pakketten door de firewall te laten passeren. Deze opdracht is ingevoerd in FWSM versie 3.2(1).

NetFlow-ondersteuning in FWSM

ondersteunt FWSM NetFlow?

Oplossing

NetFlow wordt niet ondersteund in FWSM.

Gerelateerde informatie

- Ondersteuning van Cisco Catalyst 6500 Series servicesmodule voor firewall
- Ondersteuning van Cisco Catalyst 6500 Series-switches
- Cisco 7600 Series ondersteuningspagina voor routers
- FWSM TCP-onderschepping en SYN-koekjes uitgelegd
- Technische ondersteuning en documentatie – Cisco Systems