Konfigurationsbeispiel für FWSM

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die grundlegende Konfiguration des Firewall Services Module (FWSM) konfiguriert wird, das entweder auf den Cisco Switches der Serie 6500 oder auf den Cisco Routern der Serie 7600 installiert ist. Dazu gehören die Konfiguration von IP-Adressen, Standard-Routing, statischem und dynamischem NAT, Zugriffskontrolllisten (ACLs)-Anweisungen, um den gewünschten Datenverkehr zuzulassen oder unerwünschten Datenverkehr zu blockieren, Anwendungsserver wie Websense für die Überprüfung des Internetdatenverkehrs vom internen Netzwerk aus und der Webserver für die Internetbenutzer.

Hinweis: In einem FWSM High Availability (HA)-Szenario kann das Failover nur dann erfolgreich synchronisiert werden, wenn die Lizenzschlüssel genau zwischen den Modulen identisch sind. Daher kann das Failover nicht zwischen den FWSMs mit unterschiedlichen Lizenzen funktionieren.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Firewall Services-Modul, das die Softwareversion 3.1 oder höher ausführt
- Catalyst Switches der Serie 6500 mit den folgenden erforderlichen Komponenten:Supervisor Engine mit Cisco IOS®-Software, die als Cisco IOS-Supervisor oder Catalyst-Betriebssystem (OS) bezeichnet wird. In Tabelle sind die unterstützten Supervisor Engine- und Software-Versionen aufgeführt.Multilayer Switch Feature Card (MSFC) 2 mit Cisco IOS-Software Tabelle enthält Informationen zu unterstützten Cisco IOS-Softwareversionen.

[1] Das FWSM unterstützt den Supervisor 1 oder 1A nicht.

[2] Wenn Sie Catalyst OS auf dem Supervisor verwenden, können Sie jede dieser unterstützten Cisco IOS-Softwareversionen auf der MSFC verwenden. Wenn Sie die Cisco IOS-Software auf dem Supervisor verwenden, verwenden Sie dieselbe Version auf der MSFC.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch für Cisco Router der Serie 7600 verwendet werden, wobei die erforderlichen Komponenten wie folgt dargestellt sind:

- Supervisor Engine mit Cisco IOS-Software Tabelle enthält Informationen zu unterstützten Supervisor Engine- und Cisco IOS-Softwareversionen.
- MSFC 2 mit Cisco IOS-Software Tabelle enthält Informationen zu unterstützten Cisco IOS-Softwareversionen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Das FWSM ist ein hochleistungsfähiges, platzsparendes Stateful Firewall-Modul, das in den Switches der Catalyst 6500-Serie und den Routern der Cisco 7600-Serie installiert wird.

Firewalls schützen interne Netzwerke vor nicht autorisierten Zugriffen durch Benutzer in einem externen Netzwerk. Die Firewall kann auch interne Netzwerke voneinander schützen, z. B. wenn ein Personalnetzwerk von einem Benutzernetzwerk getrennt bleibt. Wenn Sie über

Netzwerkressourcen verfügen, die einem externen Benutzer zur Verfügung stehen müssen, z. B. einem Web- oder FTP-Server, können Sie diese Ressourcen in einem separaten Netzwerk hinter der Firewall, der so genannten demilitarisierten Zone (DMZ), platzieren. Die Firewall ermöglicht einen eingeschränkten Zugriff auf die DMZ. Da die DMZ jedoch nur die öffentlichen Server umfasst, betrifft ein Angriff nur die Server und nicht die anderen internen Netzwerke. Sie können auch steuern, wann interne Benutzer auf externe Netzwerke zugreifen, z. B. den Zugriff auf das Internet, wenn Sie nur bestimmte Adressen zulassen, Authentifizierung oder Autorisierung erfordern oder sich mit einem externen URL-Filterungsserver abstimmen.

Das FWSM umfasst zahlreiche erweiterte Funktionen, z. B. mehrere Sicherheitskontexte, die virtualisierten Firewalls ähneln, eine transparente (Layer 2) Firewall oder gerouteten (Layer 3) Firewall-Betrieb, Hunderte von Schnittstellen und viele weitere Funktionen.

Während der Gespräche über Netzwerke, die mit einer Firewall verbunden sind, befindet sich das externe Netzwerk vor der Firewall, das interne Netzwerk ist geschützt und hinter der Firewall, und eine DMZ, die hinter der Firewall liegt, ermöglicht den eingeschränkten Zugriff auf externe Benutzer. Da Sie mit dem FWSM viele Schnittstellen mit unterschiedlichen Sicherheitsrichtlinien konfigurieren können, die viele interne Schnittstellen, viele DMZs und bei Bedarf sogar viele externe Schnittstellen umfassen, werden diese Begriffe nur allgemein verwendet.

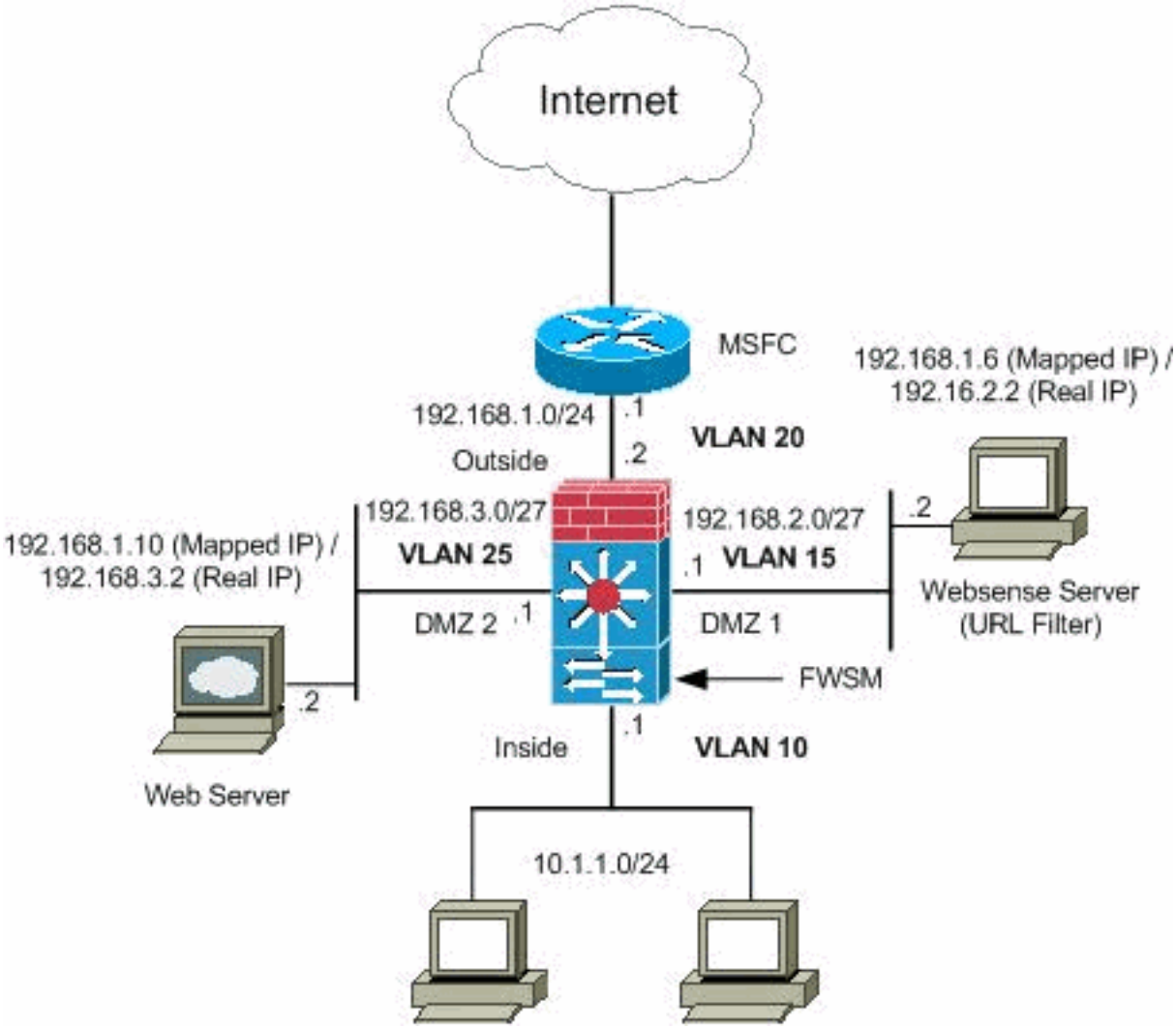
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Catalyst Switch der Serie 6500 - Konfiguration
- FWSM-Konfiguration

Catalyst Switch der Serie 6500 - Konfiguration

1. Sie können das FWSM in den Catalyst Switches der Serie 6500 oder in den Cisco Routern der Serie 7600 installieren. Die Konfiguration beider Serien ist identisch, und die Serien werden in diesem Dokument allgemein als **Switch** bezeichnet.**Hinweis:** Vor der Konfiguration von FWSM müssen Sie den Switch entsprechend konfigurieren.
2. **Zuweisen von VLANs zum Firewall Services-Modul** - In diesem Abschnitt wird beschrieben, wie Sie dem FWSM VLANs zuweisen. Das FWSM enthält keine externen physischen Schnittstellen. Stattdessen werden VLAN-Schnittstellen verwendet. Das Zuweisen von VLANs zum FWSM ähnelt der Zuweisung eines VLANs zu einem Switch-Port. Das FWSM enthält eine interne Schnittstelle zum Switch-Fabric-Modul (falls vorhanden) oder zum gemeinsamen Bus.**Hinweis:** Weitere Informationen zum Erstellen von VLANs und zum

Zuweisen von VLANs zu Switches finden Sie im Abschnitt Konfigurieren von VLANs im Catalyst 6500 Switches Software Configuration Guide.**VLAN-Richtlinien:**Sie können private VLANs mit dem FWSM verwenden. Weisen Sie dem FWSM das primäre VLAN zu. Das FWSM verarbeitet automatisch sekundären VLAN-Datenverkehr.Sie können keine reservierten VLANs verwenden.Sie können VLAN 1 nicht verwenden.Wenn Sie FWSM-Failover innerhalb desselben Switch-Chassis verwenden, weisen Sie die VLAN(s), die Sie für Failover und Stateful Communications reserviert haben, nicht einem Switch-Port zu. Wenn Sie jedoch ein Failover zwischen den Chassis verwenden, müssen Sie die VLANs in den Trunk-Port zwischen den Chassis einbinden.Wenn Sie dem Switch die VLANs nicht hinzufügen, bevor Sie sie dem FWSM zuweisen, werden die VLANs in der Supervisor Engine-Datenbank gespeichert und an das FWSM gesendet, sobald sie dem Switch hinzugefügt werden.Weisen Sie dem FWSM VLANs zu, bevor Sie diese der MSFC zuweisen.VLANs, die diese Bedingung nicht erfüllen, werden aus dem Bereich der VLANs verworfen, die Sie im FWSM zuweisen möchten.**Weisen Sie dem FWSM in der Cisco IOS-Software VLANs zu:**Erstellen Sie in der Cisco IOS-Software bis zu 16 Firewall-VLAN-Gruppen, und weisen Sie die Gruppen dann dem FWSM zu. Beispielsweise können Sie alle VLANs einer Gruppe zuweisen, eine interne Gruppe und eine externe Gruppe erstellen oder für jeden Kunden eine Gruppe erstellen. Jede Gruppe kann unbegrenzte VLANs enthalten.Sie können dasselbe VLAN nicht mehreren Firewall-Gruppen zuweisen. Sie können einem FWSM jedoch mehrere Firewall-Gruppen zuweisen und mehreren FWSMs eine Firewall-Gruppe zuweisen. VLANs, die Sie mehreren FWSMs zuweisen möchten, können sich beispielsweise in einer separaten Gruppe von VLANs befinden, die für jedes FWSM eindeutig sind.Gehen Sie wie folgt vor, um dem FWSM VLANs zuzuweisen:

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

Beim `VLAN_range` kann es sich um ein oder mehrere VLANs handeln, z. B. 2 bis 1000 und 1025 bis 4094, die entweder als eine einzige Zahl (n) wie 5, 10, 15 oder als Bereich (n-x) wie 5-10, 10-20 identifiziert werden.**Hinweis:** Geroutete Ports und WAN-Ports belegen interne VLANs, sodass VLANs im Bereich 1020-1100 möglicherweise bereits verwendet werden.**Beispiel:**

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

Führen Sie die Schritte aus, um die Firewall-Gruppen dem FWSM zuzuweisen.

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

Die `firewall_group` ist eine oder mehrere Gruppennummern, entweder eine einzelne Zahl (n) wie 5 oder ein Bereich wie 5-10.**Beispiel:**

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

Weisen Sie dem FWSM VLANs in der Catalyst-Betriebssystemsoftware zu - In der Catalyst-Betriebssystemsoftware weisen Sie dem FWSM eine Liste von VLANs zu. Sie können bei Bedarf dasselbe VLAN mehreren FWSMs zuweisen. Die Liste kann unbegrenzte VLANs enthalten.Führen Sie die Schritte aus, um dem FWSM VLANs zuzuweisen.

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

Bei der `vlan_list` kann es sich um ein oder mehrere VLANs handeln, z. B. 2 bis 1000 und 1025 bis 4094, die entweder als einzelne Nummer (n) wie 5, 10, 15 oder als Bereich (n-x)

wie 5-10, 10-20 identifiziert werden.

3. **Hinzufügen von Switched Virtual Interfaces zur MSFC** - Ein auf der MSFC definiertes VLAN wird als "Switched Virtual Interface" bezeichnet. Wenn Sie dem FWSM das für die SVI verwendete VLAN zuweisen, werden die MSFC-Routen zwischen dem FWSM und anderen Layer-3-VLANs weitergeleitet.Aus Sicherheitsgründen kann standardmäßig nur eine SVI zwischen der MSFC und dem FWSM vorhanden sein. Wenn Sie beispielsweise das System mit mehreren SVIs falsch konfigurieren, können Sie versehentlich zulassen, dass Datenverkehr durch das FWSM weitergeleitet wird, wenn Sie der MSFC sowohl interne als auch externe VLANs zuweisen.Führen Sie die Schritte aus, um die SVI zu konfigurieren

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

Beispiel:

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

Catalyst Switch der Serie 6500 - Konfiguration
`!--- 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`

Hinweis: Sitzung im FWSM vom Switch mit dem für Ihr Switch-Betriebssystem geeigneten Befehl:

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

- Catalyst OS-Software:
  ```
  Console> (enable) session module_number
  ```

(Optional) Gemeinsame Nutzung von VLANs mit anderen Dienstmodulen - Wenn der Switch über andere Dienstmodule verfügt, z. B. Application Control Engine (ACE), ist es möglich, dass Sie einige VLANs mit diesen Dienstmodulen gemeinsam nutzen müssen. Weitere Informationen zur Optimierung der FWSM-Konfiguration bei der Arbeit mit solchen anderen Modulen finden Sie unter Service Module Design with ACE und FWSM.

FWSM-Konfiguration

1. **Konfigurieren von Schnittstellen für FWSM**: Bevor Sie Datenverkehr über FWSM zulassen können, müssen Sie einen Schnittstellennamen und eine IP-Adresse konfigurieren. Sie sollten auch die Sicherheitsstufe von der Standardeinstellung (0) ändern. Wenn Sie eine Schnittstelle `innerhalb` benennen und die Sicherheitsstufe nicht explizit festlegen, legt das FWSM die Sicherheitsstufe auf 100 fest.**Hinweis:** Jede Schnittstelle muss eine Sicherheitsstufe zwischen 0 (niedrigste Stufe) und 100 (höchste Stufe) aufweisen.

Beispielsweise sollten Sie Ihr sicherstes Netzwerk, z. B. das interne Hostnetzwerk, Ebene 100 zuweisen, während das mit dem Internet verbundene externe Netzwerk die Ebene 0 sein kann. Andere Netzwerke, z. B. DMZs, können dazwischen liegen.Sie können der Konfiguration eine beliebige VLAN-ID hinzufügen, aber nur VLANs, z. B. 10, 15, 20 und 25, die dem FWSM vom Switch zugewiesen sind, können Datenverkehr weiterleiten. Verwenden Sie den Befehl **show vlan**, um alle VLANs anzuzeigen, die dem FWSM zugewiesen sind.

```
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
```

Tipp: Im **Befehl name** *<name>* ist der *Name* eine Zeichenfolge mit bis zu 48 Zeichen und es wird nicht zwischen Groß- und Kleinschreibung unterschieden. Sie können den Namen ändern, wenn Sie diesen Befehl mit einem neuen Wert erneut eingeben. Geben Sie nicht das no-Formular ein, da mit diesem Befehl alle Befehle, die auf diesen Namen verweisen, gelöscht werden.

2. **Konfigurieren Sie die Standardroute:**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

Eine Standardroute gibt die Gateway-IP-Adresse (192.168.1.1) an, an die FWSM alle IP-Pakete sendet, für die keine erfasste oder statische Route vorliegt. Eine Standardroute ist einfach eine statische Route mit 0.0.0.0/0 als Ziel-IP-Adresse. Routen, die ein bestimmtes Ziel identifizieren, haben Vorrang vor der Standardroute.

3. **Dynamic NAT** übersetzt eine Gruppe von realen Adressen (10.1.1.0/24) in einen Pool zugeordnete Adressen (192.168.1.20-192.168.1.50), die im Zielnetzwerk routbar sind. Der zugeordnete Pool kann weniger Adressen enthalten als die tatsächliche Gruppe. Wenn ein Host, den Sie übersetzen möchten, auf das Zielnetzwerk zugreift, weist das FWSM ihm eine IP-Adresse aus dem zugeordneten Pool zu. Die Übersetzung wird nur hinzugefügt, wenn der richtige Host die Verbindung initiiert. Die Übersetzung ist nur für die Dauer der Verbindung vorhanden, und ein Benutzer behält nicht die gleiche IP-Adresse, nachdem die Übersetzung abgelaufen ist.

```
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
```

Sie müssen eine ACL erstellen, um den Datenverkehr aus dem internen Netzwerk 10.1.1.0/24 in das DMZ1-Netzwerk (192.168.2.0) zu verweigern und die anderen Arten des

Datenverkehrs ins Internet über die Anwendung des ACL-*Internets* zur internen Schnittstelle als interne Richtung für eingehenden Datenverkehr zuzulassen.

4. **Statische NAT** erstellt eine feste Übersetzung von echten Adressen in zugeordnete Adressen.Bei dynamischer NAT und PAT verwendet jeder Host für jede nachfolgende Übersetzung eine andere Adresse oder einen anderen Port. Da die zugeordnete Adresse für jede Verbindung mit statischer NAT gleich ist und eine persistente Übersetzungsregel vorhanden ist, können Hosts im Zielnetzwerk mithilfe von statischer NAT Datenverkehr zu einem übersetzten Host initiieren, wenn eine Zugriffsliste vorhanden ist, die diese zulässt.Der Hauptunterschied zwischen dynamischer NAT und einem Adressbereich für statische NAT besteht darin, dass ein Remote-Host eine Verbindung zu einem übersetzten Host initiieren kann, wenn eine Zugriffsliste vorhanden ist, die dies zulässt, während dies bei dynamischer NAT nicht der Fall ist. Außerdem benötigen Sie eine identische Anzahl zugeordneter Adressen als echte Adressen mit statischer 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
```

Dies sind die beiden angezeigten statischen NAT-Anweisungen. Die erste ist dafür vorgesehen, die tatsächliche IP 192.168.2.2 auf der internen Schnittstelle in die zugeordnete IP 192.168.1.6 auf dem externen Subnetz zu übersetzen, sofern die ACL den Datenverkehr von der Quelle 192.168.1.30 zur zugeordneten IP 192.168 zulässt. 1.6, um auf den Websense-Server im DMZ1-Netzwerk zuzugreifen. Ebenso wurde mit der zweiten statischen NAT-Anweisung das tatsächliche IP 192.168.3.2 auf der internen Schnittstelle in das zugeordnete IP 192.168.1.10 auf dem externen Subnetz übersetzt, vorausgesetzt, dass die ACL den Datenverkehr vom Internet zum zugeordneten IP 192.168.1.10 zulässt, um auf das Web zuzugreifen -Server im DMZ2-Netzwerk verwenden und die UDP-Portnummer im Bereich von 8766 bis 3000 liegen.

5. Der **url-server-**Befehl gibt den Server an, auf dem die Websense-URL-Filteranwendung ausgeführt wird. Das Limit ist 16 URL-Server im Einzelkontext-Modus und vier URL-Server im Multi-Mode. Sie können jedoch jeweils nur eine Anwendung, entweder N2H2 oder Websense, verwenden. Wenn Sie außerdem die Konfiguration auf der Sicherheits-Appliance ändern, wird die Konfiguration auf dem Anwendungsserver nicht aktualisiert. Dies muss entsprechend den Anweisungen des Anbieters separat erfolgen.Der Befehl **url-server** muss konfiguriert werden, bevor Sie den Befehl **filter** für HTTPS und FTP eingeben. Wenn alle URL-Server aus der Serverliste entfernt werden, werden alle Filterbefehle für die URL-Filterung ebenfalls entfernt.Wenn Sie den Server festgelegt haben, aktivieren Sie den URL-Filterdienst mit dem Befehl **filter url**.

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

Der **Filter-URL**-Befehl ermöglicht die Verhinderung des Zugriffs von ausgehenden Benutzern aus World Wide Web-URLs, die Sie mit der Websense-Filteranwendung festgelegt haben.

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

FWSM-Konfiguration

```
!--- 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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle.

Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

1. Zeigen Sie die Modulinformationen in Übereinstimmung mit Ihrem Betriebssystem an, um sicherzustellen, dass der Switch das FWSM bestätigt und online gestellt hat: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 OS-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
```

   Hinweis: Der Befehl **show module** zeigt sechs Ports für das FWSM an. Dies sind interne Ports, die als EtherChannel gruppiert werden.

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. Geben Sie den Befehl für Ihr Betriebssystem ein, um die aktuelle Bootpartition anzuzeigen:Cisco IOS-Software:

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

   Beispiel:

```
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-Software:

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

   Beispiel:

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

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

1. **Einstellen der Standard-Boot-Partition** - Standardmäßig startet das FWSM von der Anwendungspartition **cf:4**. Sie können aber auch von der Anwendungspartition **cf:5** oder in die Wartungspartition **cf:1** booten. Um die Standard-Boot-Partition zu ändern, geben Sie den Befehl für Ihr Betriebssystem ein:Cisco IOS-Software:
   ```
   Router(config)#boot device module mod_num cf:n
   ```

   Dabei ist n 1 (Wartung), 4 (Anwendung) oder 5 (Anwendung).Catalyst OS-Software:
   ```
   Console> (enable) set boot device cf:n mod_num
   ```

   Dabei ist n 1 (Wartung), 4 (Anwendung) oder 5 (Anwendung).
2. **Zurücksetzen des FWSM in der Cisco IOS-Software** - Geben Sie den folgenden Befehl ein, um das FWSM zurückzusetzen:
   ```
   Router#hw-module module mod_num reset [cf:n] [mem-test-full]
   ```

   Das **cf:n-**Argument ist die Partition, entweder 1 (Wartung), 4 (Anwendung) oder 5 (Anwendung). Wenn Sie die Partition nicht angeben, wird die Standardpartition verwendet, die in der Regel **cf:4 lautet**.Die **mem-test-full-**Option führt einen vollständigen Speichertest aus, der ca. sechs Minuten in Anspruch nimmt.**Beispiel:**
   ```
   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 ...
   ```
   Für **Catalyst OS** Software:
   ```
   Console> (enable) reset mod_num [cf:n]
   ```

   Dabei ist **cf:n** die Partition, entweder 1 (Wartung), 4 (Anwendung) oder 5 (Anwendung). Wenn Sie die Partition nicht angeben, wird die Standardpartition verwendet, die in der Regel **cf:4 lautet**.

Hinweis: NTP kann nicht für FWSM konfiguriert werden, da es seine Einstellungen vom Switch bezieht.

Problem: Der VLAN-Datenverkehr vom FWSM konnte nicht an den IPS-Sensor 4270 weitergeleitet werden.

Sie können den Datenverkehr von FWSM nicht an die IPS-Sensoren weiterleiten.

Lösung

Um den Datenverkehr durch das IPS zu erzwingen, besteht der Trick darin, ein zusätzliches VLAN zu erstellen, um eines Ihrer aktuellen VLANs effektiv in zwei zu unterteilen und sie dann

miteinander zu verbinden. In diesem Beispiel werden VLAN 401 und 501 vorgestellt, um Folgendes zu verdeutlichen:

- Wenn Sie den Datenverkehr in **VLAN 401** scannen möchten, erstellen Sie ein anderes VLAN **VLAN 501** (zusätzliches VLAN). Deaktivieren Sie dann die VLAN-Schnittstelle 401, die die Hosts in 401 derzeit als Standard-Gateway verwenden.
- Aktivieren Sie anschließend die VLAN 501-Schnittstelle mit der *gleichen* Adresse, die Sie zuvor für die VLAN 401-Schnittstelle deaktiviert haben.
- Platzieren Sie eine der IPS-Schnittstellen in VLAN 401, die andere in VLAN 501.

Sie müssen lediglich das Standard-Gateway für VLAN 401 auf VLAN 501 verschieben. Falls vorhanden, müssen Sie die gleichen Änderungen für VLANs vornehmen. Beachten Sie, dass VLANs im Wesentlichen wie LAN-Segmente sind. Sie können ein Standard-Gateway auf einem anderen Kabelteil als die Hosts haben, die es verwenden.

Problem mit Out-of-Order-Paketen im FWSM

Wie kann ich das Problem bei Out-of-Order-Paketen in FWSM lösen?

Lösung

Geben Sie den Befehl sysopt np complete-unit **im globalen Konfigurationsmodus aus, um das Problem mit Out-of-Order-Paketen in FWSM zu beheben.** Dieser Befehl wurde in FWSM Version 3.2(5) eingeführt und stellt sicher, dass Pakete in der gleichen Reihenfolge weitergeleitet werden, in der sie empfangen wurden.

Problem: Asymmetrisch geroutete Pakete können nicht über die Firewall weitergeleitet werden.

Sie können asymmetrisch geroutete Pakete nicht über die Firewall weiterleiten.

Lösung

Geben Sie den Befehl set connection advanced-options tcp-state-bypass-bypass **im Klassenkonfigurationsmodus aus, um asymmetrisch geroutete Pakete durch die Firewall zu leiten.** Dieser Befehl wurde in FWSM Version 3.2(1) eingeführt.

NetFlow-Unterstützung in FWSM

Unterstützt FWSM Netflow?

Lösung

NetFlow wird in FWSM nicht unterstützt.

Zugehörige Informationen

- Support-Seite für Cisco Catalyst Firewall Services Module der Serie 6500
- Support-Seite für Cisco Catalyst Switches der Serie 6500

- Support-Seite für Cisco Router der Serie 7600
- Erläuterung des FWSM-TCP-Abfangen und der SYN-Cookies
- Technischer Support und Dokumentation - Cisco Systems