FWSM： マルチ コンテキストの設定例

目次

概要

このドキュメントでは、ファイアウォール サービス モジュール（FWSM）のマルチ コンテキストの設定に使用される手順について説明します。

単一の FWSM は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。 各コンテキストにはそれぞれのセキュリティ ポリシー、インターフェイス、および管理者が存在します。 マルチ コンテキストは、複数のスタンドアロン デバイスと同様です。 マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、および管理を含む多くの機能がサポートされています。 ダイナミック ルーティング プロトコルを含む、一部の機能はサポートされていません。

次のような状況で、マルチ セキュリティ コンテキストを使用できます。

- サービス プロバイダーとして、多くの顧客にセキュリティ サービスを販売しようとしている場合。 FWSM でマルチ セキュリティ コンテキストを有効にすると、すべての顧客のトラフィックの分離と安全を維持し、設定を容易にする、コスト効率に優れた、スペース節約型のソリューションを実装できます。
- 大企業または大学キャンパスで、すべての部門の完全な独立性を維持する場合。
- 企業で部門ごとに異なるセキュリティ ポリシーを適用しようとしている場合。
- 複数のファイアウォールを必要とするネットワークを所有している場合。

「PIX/ASA 7.x 以降： マルチ コンテキストの設定例」を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 3.2(5) が稼働する Firewall Service Module (FWSM; ファイアウォール サービス モジュール) に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

コンテキスト コンフィギュレーション ファイル

コンテキスト コンフィギュレーション

FWSM は、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイス上で設定できるほぼすべてのオプションを特定する各コンテキスト用の設定を含んでいます。 コンテキスト コンフィギュレーションは、内部のフラッシュ メモリまたは外部のフラッシュ メモリ カードに格納することも、TFTP、FTP、または HTTP (S) サーバからダウンロードすることもできます。

システム設定

システム管理者は、シングルモード コンフィギュレーションでのスタートアップ コンフィギュレーションとなるシステム コンフィギュレーション中でコンテキストごとのコンフィギュレーションの保存場所、割り当てるインターフェイス、その他のコンテキストオペレーティングのためのパラメータなどの設定を用いて、コンテキストの追加と管理を行います。 システム コンフィギュ

レーションは、FWSM の基本的な設定を特定します。 システム コンフィギュレーションには、ネットワーク インターフェイスやそれ自体のネットワーク設定は含まれません。 システムがネットワーク リソースにアクセスすることが必要な場合は（サーバからのコンテキストをダウンロードするなど）、管理コンテキストとして指定されるコンテキストの 1 つを使用します。 システム コンフィギュレーションは、フェールオーバー トラフィック専用の特別なフェールオーバー インターフェイスを含んでいます。

管理コンテキストの設定

管理コンテキストはその他のコンテキストと似ていますが、ユーザが管理コンテキストにログインすると、ユーザはシステム管理者権限を持つようになり、システムと他のすべてのコンテキストにアクセスできる点が異なっています。 管理コンテキストはまったく制限がなく、通常のコンテキストとして使用できます。 ただし、管理コンテキストにログインすると、ユーザにはすべてのコンテキストに対する管理者権限が付与されるため、管理コンテキストへのアクセスは適切なユーザに制限する必要がある場合があります。 管理コンテキストは、フラッシュ メモリ上に存在する必要があり、リモートに存在することはできません。

システムがすでにマルチ コンテキスト モードである場合、またはシングル モードから変換した場合、管理コンテキストは、admin.cfg という名前の内部フラッシュ メモリ上のファイルとして自動的に作成されます。 このコンテキストの名前は admin です。 管理コンテキストとして admin.cfg を使用したくない場合は、管理コンテキストを変更できます。

サポートされない機能

マルチ コンテキスト モードでは、次の機能はサポートされていません。

- ダイナミック ルーティング プロトコルセキュリティ コンテキストでサポートされているのはスタティック ルートだけです。 マルチ コンテキスト モードでは OSPF や RIP を有効にできません。
- マルチキャスト

セキュリティ コンテキストへの管理アクセス

FWSM は、マルチ コンテキスト モードのシステム管理者アクセスだけでなく、個別のコンテキスト管理者向けのアクセスも提供します。 以降のセクションでは、システム管理者として、またはコンテキスト管理者としてログインすることについて説明します。

システム管理者のアクセス

次の 2 つの方法で、システム管理者として FWSM にアクセスできます。

- スイッチから FWSM へのセッション。スイッチから、システム実行スペースにアクセスします。
- Telnet、SSH、または ASDM を使用した管理コンテキストへのアクセス。Telnet、SSH、および ASDM アクセスを有効にする方法についての詳細は、「管理アクセスの設定」を参照してください。

システム管理者は、すべてのコンテキストにアクセスできます。

管理コンテキスト、もしくはシステム コンテキストから他のコンテキストに変更した場合、ユーザ名はデフォルトの enable_15 ユーザ名に変わります。 そのコンテキストでコマンド認可を設定

した場合、enable_15 ユーザの認可権限を設定する必要があります。または、そのコンテキストのコマンド認可設定で十分な権限を提供する対象である別の名前でログインする方法もあります。 **login** コマンドを入力して、ユーザ名でログインします。 たとえば、ユーザ名 admin を使用して管理コンテキストにログインします。 管理コンテキストにはコマンド認可コンフィギュレーションはありませんが、他のすべてのコンテキストにはコマンド認可が含まれています。 また、利便性のために、各コンテキスト コンフィギュレーションは、最大の権限を持つユーザ admin を含んでいるとします。 この場合、管理コンテキストから context A に変更した場合、ユーザ名が変化するため、**login** コマンドを入力する際に admin として再度ログインする必要があります。 また、context B に変更した場合、**login** コマンドを再度入力して、admin としてログインする必要があります。

システム実行スペースは AAA コマンドをサポートしていませんが、ローカル データベースのユーザ名と独自のイネーブル パスワードを設定して、個人としてログインできます。

コンテキスト管理者アクセス

Telnet、SSH、または ASDM でコンテキストにアクセスできます。 管理コンテキスト以外にログインした場合、アクセスできるのはそのコンテキスト用のコンフィギュレーションだけです。 そのコンテキストへの個別のログインを提供できます。

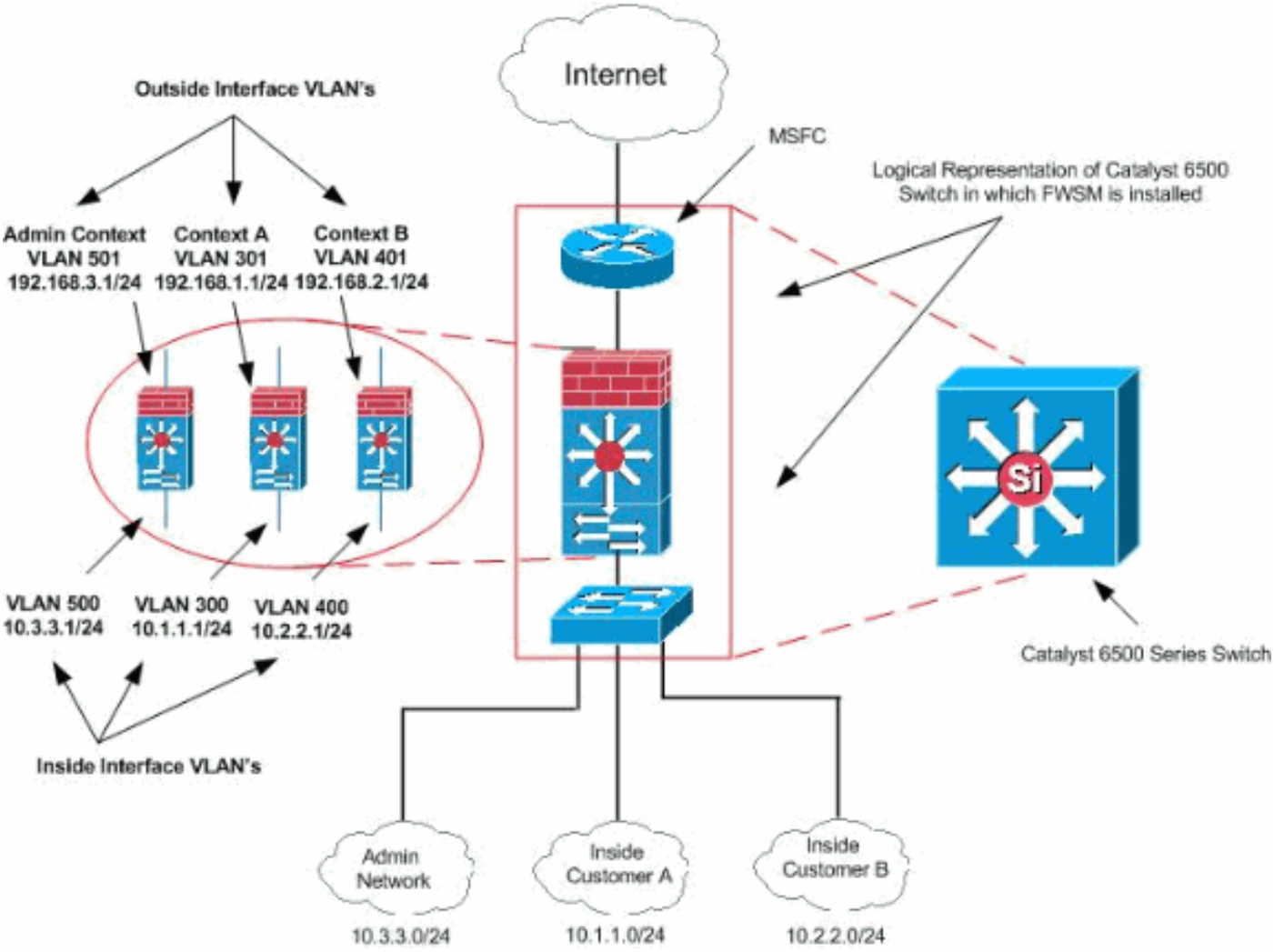
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



マルチ コンテキスト モードのイネーブル化とディセーブル化

Cisco に FWSM を発注した方法によっては、ご使用の FWSM はすでにマルチ セキュリティ コンテキスト用に設定されている場合があります。 ただし、アップグレードする場合は、このセクションの手順に従って、シングル モードからマルチ モードに変換する必要がある場合があります。 ASDM はモードの変更をサポートしていないため、モードを変更には CLI を使用する必要があります。

シングル モード コンフィギュレーションのバックアップ

シングル モードからマルチ モードに変換する際には、FWSM が実行コンフィギュレーションを 2 つのファイルに変換します。 元のスタートアップ コンフィギュレーションは保存されないため、元のスタートアップ コンフィギュレーションが実行コンフィギュレーションと異なる場合は、先に進む前にバックアップする必要があります。

マルチ コンテキスト モードの有効化

リブートを経た場合でも、コンテキスト モード (シングルまたはマルチ) はコンフィギュレーション ファイルには保存されません。 コンフィギュレーションを別のデバイスにコピーする必要がある場合は、**mode** コマンドで、新しいデバイス上のモードを設定して一致させます。

シングル モードからマルチ モードに変換する際には、FWSM が実行コンフィギュレーションを 2 つのファイルに変換します。

1. システム コンフィギュレーションを構成する新しいスタートアップ コンフィギュレーション
2. 内部フラッシュ メモリのルート ディレクトリの管理コンテキストを構成する admin.cfg

元の実行コンフィギュレーションは、(内部フラッシュ メモリのルート ディレクトリに) old_running.cfg として保存されます。 元のスタートアップ コンフィギュレーションは保存されません。 FWSM は、管理コンテキストのエントリをシステム コンフィギュレーションに名前「admin」で自動的に追加します。

次のコマンドを入力して、マルチ モードを有効にします。

```
hostname(config)#mode multiple
```

FWSM をリブートするかどうかを確認するダイアログが表示されます。

```
FWSM(config)#mode multiple WARNING: This command will change the behavior of the device WARNING:
This command will initiate a Reboot Proceed with change mode? [confirm] Convert the system
configuration? [confirm] ! The old running configuration file will be written to flash The admin
context configuration will be written to flash The new running configuration file was written to
flash Security context mode: multiple *** *** --- SHUTDOWN NOW --- *** *** Message to all
terminals: *** *** change mode Rebooting.... Booting system, please wait... * * !--- Output
suppressed * * INFO: Admin context is required to get the interfaces *** Output from config line
20, "arp timeout 14400" Creating context 'admin'... Done. (1) *** Output from config line 23,
"admin-context admin" Cryptochecksum (changed): a219baf3 037b31b4 09289829 1ab9790a *** Output
from config line 25, " config-url flash:/admi..." Cryptochecksum (changed): d4f0451b 405720e1
bbccf404 86be061c Type help or '?' for a list of available commands. FWSM>
```

リブート後は、次が FWSM のデフォルト コンフィギュレーションになります。

FWSM のデフォルト コンフィギュレーション

```
FWSM#show running-config : Saved : FWSM Version 3.2(5)5
<system> ! resource acl-partition 12 hostname FWSM
domain-name default.domain.invalid enable password
8Ry2YjIyt7RRXU24 encrypted ! interface Vlan501 !
interface Vlan502 ! passwd 2KFQnbNIdI.2KYOU encrypted
class default limit-resource IPSec 5 limit-resource Mac-
addresses 65535 limit-resource ASDM 5 limit-resource SSH
5 limit-resource Telnet 5 limit-resource All 0 ! ftp
mode passive gdb enable pager lines 24 no failover no
asdm history enable arp timeout 14400 console timeout 0
admin-context admin context admin allocate-interface
Vlan501 allocate-interface Vlan502 config-url
disk:/admin.cfg !--- admin context is created !--- by
default once you enable !--- multiple mode ! prompt
hostname context
Cryptochecksum:d62411d2a15f1da35c76fe071b61dcdb : end
FWSM#
```

セキュリティ コンテキストの設定

システム コンフィギュレーションのセキュリティ コンテキスト定義が、コンテキスト名、コンフィギュレーション ファイルの URL、コンテキストで使用できるインターフェイス、およびその他のコンテキスト パラメータを特定します。

注: 管理コンテキストがない場合 (コンフィギュレーションをクリアした場合など) 、次のコマンドを入力するときに、最初に管理コンテキスト名を指定する必要があります。

```
hostname(config)#admin-context <name>
```

注: まだこのコンテキスト名はコンフィギュレーションに存在しませんが、引き続き **context name** コマンドを入力すると、指定した名前を照合して管理コンテキスト コンフィギュレーションを継続できます。

システム コンフィギュレーションでコンテキストを追加または変更するには、次の手順を実行します。

1. コンテキストの追加または変更を行うには、**システム実行スペースで次のコマンドを入力します。**
   hostname(config)#context <name> 名前は 32 文字までの文字列です。 この名前は大文字と小文字を区別するので、たとえば、「customerA」と「CustomerA」という名前の 2 つのコンテキストが共存できます。 文字、数字、またはハイフンを使用できますが、名前の最初または最後をハイフンにすることはできません。「System」と「Null」（大文字と小文字の両方）は予約名なので使用できません。
2. （オプション）このコンテキストに説明を追加するには、次のコマンドを入力します。
   hostname(config-ctx)#description *text*
3. 次のコマンドを入力して、コンテキストで使用できるインターフェイスを指定します。
   hostname(config-ctx)#allocate-interface vlannumber[-vlannumber] [map_name[-map_name] [invisible | visible]] このコマンドを複数回入力することで、異なった複数の範囲を指定できます。 このコマンドの **no** 形式を使用して割り当てを削除すると、このインターフェイスが含まれるコンテキスト コマンドが実行コンフィギュレーションから削除されます。 VLAN 番号または VLAN の範囲（通常は 2 ~ 1000 と 1025 ~ 4094）を入力します。 サポートされている VLAN については、スイッチのドキュメントを参照してください。 **show vlan** コマンドを使用して、FWSM に割り当てられた VLAN のリストを参照してください。 まだ FWSM に割り当てられていない VLAN を割り当てることができますが、VLAN でトラフィックを通過させるには、スイッチから VLAN を割り当てる必要があります。 インターフェイスを割り当てると、FWSM は、システム コンフィギュレーションで各 VLAN について **interface** コマンドを自動的に追加します。
4. 次のコマンドを入力して、システムがコンテキスト コンフィギュレーションをダウンロードする元である URL を特定します。hostname(config-ctx)#**config-url url** コンテキストの URL を追加すると、コンフィギュレーションが利用可能な場合、システムは即座にコンテキストをロードして、コンテキストが実行されます。**注: allocate-interface** コマンドを入力してから **config-url** コマンドを入力してください。 FWSM は、コンテキスト コンフィギュレーションをロードする前にコンテキストにインターフェイスを割り当てる必要があります。 コンテキスト コンフィギュレーションには、インターフェイスを参照するコマンド（interface、nat、global など）を含めることができます。 最初に **config-url** コマンドを入力すると、FWSM は即座にコンテキスト コンフィギュレーションをロードします。 コンテキストがインターフェイスを参照するコマンドを含んでいる場合、そのようなコマンドは失敗します。

このシナリオでは、表の手順を実行して、マルチ コンテキストを設定します。

Customer A と Customer B という 2 人のカスタマーがいます。この場合、Customer A 用の Context A、Customer B 用の Context B、および FWSM のコンテキストを管理するための管理コンテキストなど、1 つの FWSM モジュールで 3 つのマルチ コンテキスト（実体は 3 つの FWSM）を作成します。

注: FWSM で使用する前に、Catalyst 6500 シリーズ スイッチで VLAN 300、301、400、401、500 および 501 を作成します。

次に示すように、システム実行スペースでコンテキストを作成し、作成された各コンテキストに

それぞれの VLAN を割り当て、各コンテキストの URL パスを設定します。

FWSM：マルチ コンテキストの設定手順

```
FWSM(config)#context admin FWSM(config-ctx)#allocate-
interface VLAN500 FWSM(config-ctx)#allocate-interface
VLAN501 FWSM(config-ctx)#config-url disk:/admin.cfg !---
Allocate VLAN 500 and 501 to admin context
FWSM(config)#context contextA !--- Customer A Context as
Context A FWSM(config-ctx)#allocate-interface VLAN300
FWSM(config-ctx)#allocate-interface VLAN301 !---
Allocate VLAN 300 and 301 to admin context FWSM(config-
ctx)#config-url disk:/contextA.cfg WARNING: Could not
fetch the URL disk:/contextA.cfg INFO: Creating context
with default config !--- To identify the URL from which
the !--- system downloads the context configuration.
FWSM(config-ctx)#context contextB Creating context
'contextB'... Done. (3) !--- Customer B Context as
Context B FWSM(config-ctx)#allocate-interface VLAN400
FWSM(config-ctx)#allocate-interface VLAN401 !---
Allocate VLAN 400 and 401 to admin context FWSM(config-
ctx)#config-url disk:/contextB.cfg WARNING: Could not
fetch the URL disk:/contextB.cfg INFO: Creating context
with default config FWSM(config-ctx)#exit
```

FWSM： システム実行スペースの設定

FWSM： システム実行スペースの設定

```
FWSM(config)#show running-config : Saved : FWSM Version
3.2(5)5 <system> ! resource acl-partition 12 hostname
FWSM domain-name default.domain.invalid enable password
8Ry2YjIyt7RRXU24 encrypted ! interface Vlan300 !
interface Vlan301 ! interface Vlan400 ! interface
Vlan401 ! interface Vlan501 ! interface Vlan502 ! passwd
2KFQnbNIdI.2KYOU encrypted class default limit-resource
IPSec 5 limit-resource Mac-addresses 65535 limit-
resource ASDM 5 limit-resource SSH 5 limit-resource
Telnet 5 limit-resource All 0 ! ftp mode passive gdb
enable pager lines 24 no failover no asdm history enable
arp timeout 14400 console timeout 0 admin-context admin
context admin allocate-interface Vlan501 allocate-
interface Vlan502 config-url disk:/admin.cfg ! context
contextA allocate-interface Vlan300 allocate-interface
Vlan301 config-url disk:/contextA.cfg ! context contextB
allocate-interface Vlan400 allocate-interface Vlan401
config-url disk:/contextB.cfg ! prompt hostname context
Cryptochecksum:d62411d2a15f1da35c76fe071b61dcdb : end
FWSM#
```

コンテキストとシステム実行スペースの変更

システム実行スペース（または Telnet または SSH を使用して管理コンテキスト）にログインすると、コンテキストを変更し、各コンテキスト内で設定と監視のタスクを実行できます。 コンフィギュレーション モードでユーザが編集するランニング コンフィギュレーション、または **copy** または **write** コマンドの対象となるランニング コンフィギュレーションは、場所により異なります。 システム実行スペース内にいるとき、実行コンフィギュレーションは、システム コンフィギュレーションだけで構成されます。 コンテキスト内にいるとき、実行コンフィギュレーションは、そのコンテキストだけで構成されます。 たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システムとすべてのコンテキスト）は表示できません

。 表示されるのは現在のコンフィギュレーションだけです。 ただし、**write memory all** コマンドを使用すると、システム実行スペースから、すべてのコンテキストの実行コンフィギュレーションを保存できます。

システム実行スペースとコンテキストの間で変更する、または、コンテキストの間を変更するには、次のコマンドを確認してください。

- 特定のコンテキストに変更するには、次のコマンドを入力します。`hostname#`**`changeto context <context name>`** プロンプトは次のように変わります。
  `hostname/name#`
- 次のコマンドを入力して、システム実行スペースに変更します。`hostname/admin#`**`changeto system`** プロンプトは次のように変わります。
  `hostname#`

FWSM：ContextA の設定

contextA に変更し、次の手順を実行して、contextA を設定します。

!--- From the system execution space, !--- enter the ***changeto context contextA*** *command !--- in order to configure the contextA configuration.* **FWSM(config)#changeto context contextA**
FWSM/context1(config)#

FWSM：ContextA のデフォルト設定
FWSM/contextA(config)#**show running-config** *!--- Default configuration of the context1* : Saved : **FWSM Version 3.2(5)5 <context>** ! hostname contextA enable password 8Ry2YjIyt7RRXU24 encrypted names ! **interface Vlan300** no nameif no security-level no ip address ! **interface Vlan301** no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted gdb enable pager lines 24 mtu inside 1500 mtu outside 1500 no asdm history enable arp timeout 14400 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 1:00:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute no snmp-server location no snmp-server contact telnet timeout 5 ssh timeout 5 ! class-map inspection_default match default-inspection-traffic ! ! policy-map global_policy class inspection_default inspect dns maximum-length 512 inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect skinny inspect smtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global Cryptochecksum:00000000000000000000000000000000 : end FWSM/contextA# no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted gdb enable pager lines 24 no asdm history enable arp timeout 14400 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 1:00:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute no snmp-server location no snmp-server contact telnet timeout 5 ssh timeout 5 ! class-map inspection_default match default-inspection-traffic ! ! policy-map global_policy class inspection_default inspect dns maximum-length 512 inspect ftp inspect h323

```
h225 inspect h323 ras inspect netbios inspect rsh
inspect skinny inspect smtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global
Cryptochecksum:00000000000000000000000000000000 : end
```

インターネットに接続するための Customer A の設定

FWSM： ContextA の設定

```
FWSM/contextA(config)#interface vlan300
FWSM/contextA(config-if)#nameif inside WARNING: VLAN
*300* is not configured. INFO: Security level for
"inside" set to 100 by default. Access Rules Download
Complete: Memory Utilization: 1% FWSM/contextA(config-
if)#ip address 10.1.1.1 255.255.255.0
FWSM/contextA(config-if)#no shut FWSM/contextA(config-
if)#interface vlan 301 FWSM/contextA(config-if)#nameif
outside INFO: Security level for "outside" set to 0 by
default. Access Rules Download Complete: Memory
Utilization: 1% FWSM/contextA(config-if)#ip add
192.168.1.1 255.255.255.0 FWSM/contextA(config-if)#no
shut FWSM/contextA(config)#access-list outbound permit
ip any any FWSM/contextA(config)#nat (inside) 1 access-
list outbound FWSM/contextA(config)#global (outside) 1
interface INFO: outside interface address added to PAT
pool FWSM/contextA(config)#route outside-context1
0.0.0.0 0.0.0.0 192.168.1.5 FWSM/contextA(config)#exit
```

FWSM：ContextA の設定

```
FWSM/contextA#show running-config : Saved : FWSM Version
3.2(5)5 <context> ! hostname contextA enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Vlan300
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface Vlan301 nameif outside
security-level 0 ip address 192.168.1.1 255.255.255.0 !
passwd 2KFQnbNIdI.2KYOU encrypted access-list outbound
extended permit ip any any gdb enable pager lines 24 mtu
inside 1500 mtu outside 1500 no asdm history enable arp
timeout 14400 global (outside) 1 interface nat (inside)
1 access-list outbound route outside 0.0.0.0 0.0.0.0
192.168.1.5 1 !--- Output Suppressed ! class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect skinny inspect smtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global
Cryptochecksum:00000000000000000000000000000000 : end
FWSM/contextA#
```

FWSM：ContextB の設定

インターネットに接続するための Customer B の設定

contextA から contextB に変更して、contextB を設定します。

```
!--- From the system execution space, enter !--- the changeto context contextB command --- in
orderto configure the contextB configuration. FWSM/contextA(config)#changeto context contextB
```

```
FWSM/contextB(config)#
```

FWSM：ContextB の設定

```
FWSM/contextB(config)#show running-config : Saved : FWSM
Version 3.2(5)5 <context> ! hostname contextB enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
Vlan400 nameif inside security-level 100 ip address
10.2.2.1 255.255.255.0 ! interface Vlan401 nameif
outside security-level 0 ip address 192.168.2.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted
access-list outbound extended permit ip any any gdb
enable pager lines 24 mtu inside 1500 mtu outside 1500
no asdm history enable arp timeout 14400 global
(outside) 1 interface nat (inside) 1 access-list
outbound route outside 0.0.0.0 0.0.0.0 192.168.2.5 1 !--
- Output Suppressed ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect skinny inspect smtp inspect
sqlnet inspect sunrpc inspect tftp inspect sip inspect
xdmcp ! service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000 : end
FWSM/contextB(config)#
```

同様に、管理コンテキストを設定し、Inside と Outside のインターフェイスから FWSM とそのコンテキストを管理します。

マルチ コンテキスト モードでのコンフィギュレーションの変更の保存

それぞれのコンテキスト（およびシステム）コンフィギュレーションは別々に保存することも、すべてのコンテキスト コンフィギュレーションを同時に保存することもできます。 ここでは次の項目について説明します。

各コンテキストとシステムの個別保存

システムまたはコンテキストのコンフィギュレーションを保存するには、システムまたはコンテキスト内で次のコマンドを入力します。

```
hostname#write memory
```

注: copy running-config startup-config コマンドは **write memory** コマンドと同等です。

マルチ コンテキスト モードでは、コンテキストのスタートアップ コンフィギュレーションを外部サーバ上に配置できます。 この場合、セキュリティ アプライアンスは、ユーザがコンテキスト URL で特定したサーバに設定を保存して戻します。ただし、サーバに設定を保存できない HTTP または HTTPS URL を除きます。

すべてのコンテキスト コンフィギュレーションの同時保存

システム コンフィギュレーションだけでなく、すべてのコンテキストのコンフィギュレーションを同時に保存するには、システム実行スペースで次のコマンドを入力します。

```
hostname#write memory all [/noconfirm]
```

/noconfirm キーワードを入力しない場合は、次のプロンプトが表示されます。

```
Are you sure [Y/N]:
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show context**：さまざまなコンテキストを表示します。`FWSM(config)#show context Context Name Class Interfaces Mode URL *admin default Vlan501,Vlan502 Routed disk:/admin.cfg contextA default Vlan300,Vlan301 Routed disk:/contextA.cfg contextB default Vlan400,Vlan401 Routed disk:/contextB.cfg Total active Security Contexts: 3`
- **show mode**：FWSM がシングルまたはマルチ モードとして設定されていることを確認します。`FWSM(config)#show mode Security context mode: multiple The flash mode is the SAME as the running mode.`

トラブルシューティング

シングル コンテキスト モードの復元

マルチ モードからシングル モードに変換する場合、最初にスタートアップ コンフィギュレーションをすべて（可能な場合）FWSM にコピーすることができます。 マルチ モードから継承したシステム コンフィギュレーションは、シングル モード デバイスの場合は完全に機能するコンフィギュレーションではありません。 そのシステム コンフィギュレーションには設定の一部としてネットワーク インターフェイスがないため、コンソールからセキュリティ アプライアンスにアクセスして、コピーを実行する必要があります。

システム実行スペースで次の手順を実行して、古い実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーし、モードをシングル モードに変更します。

1. オリジナルの実行コンフィギュレーションのバックアップ バージョンを現在のスタートアップ コンフィギュレーションにコピーするには、システム実行スペースで次のコマンドを入力します。`hostname(config)#copy flash:old_running.cfg startup-config`
2. システム実行スペースで次のコマンドを入力して、モードをシングル モードに設定します。`hostname(config)#mode single`

FWSM がリブートします。

セキュリティ コンテキストのリロード

コンテキストのリロードは 2 つの方法で行うことができます。

1. 実行コンフィギュレーションをクリアし、スタートアップ コンフィギュレーションをインポートします。この操作により、接続や NAT テーブルなど、コンテキストと関連付けられている大部分の属性がクリアされます。
2. システム コンフィギュレーションからコンテキストを削除します。この操作は、メモリ割り当てなどの追加属性をクリアするため、トラブルシューティングに有効な場合があります。 ただし、コンテキストをシステムに追加し直すために、URL とインターフェイスを再設定する必要があります。

ここでは次の項目について説明します。

- 設定のクリアによるリロード
- コンテキストの削除と読み取りによるリロード

コンテキストの名前変更

マルチ コンテキスト モードでは、設定を変更することなくコンテキストの名前を変更することはサポートされていません。

コンフィギュレーションをファイアウォール コンフィギュレーションとして保存できますが、コンフィギュレーション全体を新しいコンテキスト名にコピーし、古いコンテキストのコンフィギュレーションを削除する必要があります。

コンテキストの削除

次のコマンドを使用して、コンテキストを削除します。 システム実行スペースから、次のコマンドを発行します。

no context contA

また、必ずコンテキストに対応する設定ファイルを削除します。

```
dir disk:

delete disk:/contA.cfg
```

関連情報

- FWSM 基本設定の例
- PIX/ASA 7.x 以降： マルチ コンテキストの設定例
- テクニカルサポートとドキュメント - Cisco Systems