株式会社レップワン
Rep1 Corp

SAMPLE

株式会社 XXXXX 御中

ファイアーウォール・侵入検知システム 設計書

作成者：株式会社レップワン

作成日時：2011/xx/xx

更新日時：2011/xx/xx

目次

本書の目的

本書は、株式会社 XXXXX 様の社内ネットワークに設置される Cisco ASA5520 を使用したファイアーウォール・侵入検知システム及びリモートアクセスサービスについて、要件要求に基づき株式会社レップワンが設計を実施した内容を記述する。

※本書のパラメーター項目やパラメーター値の記述は、Cisco ASA5500 シリーズの GUI 管理ツールである ASDM 上の表示を引用して、記載する。

1. 基本情報

1-1. 提供する機能（基本設計ポリシーの明記）

1-2. ハードウェアスペック

本システムに使用する機器のハードウェアスペックを以下に示す。

項目	アクティブ機	スタンバイ機
ホスト名	FW1	FW2
機器名	Cisco ASA5520	Cisco ASA5505
機器タイプ	セキュリティアプライアンス	セキュリティアプライアンス
システム フラッシュ	256MB	128MB
メモリ	512MB	256MB
ファイアーウォールスループット	最大 450 Mbps	最大 150 Mbps
VPN のスループット	最大 225Mbps	最大 100 Mbps
同時セッション数	280,000	1000
インターフェイス	10BASE-T / 100BASE-TX / 1000BASE-T ×4 管理用 10BASE-T / 100BASE-TX×1	10BASE-T / 100BASE-TX ×8
冗長化機能	アクティブ/アクティブ構成 アクティブ/スタンバイ構成	未サポート
電源電圧	100 ～ 240 VAC	100 ～ 240 VAC
定格出力 / 最大出力	150 W / 190 W	20W/96W
シリアルナンバー	XXXXXXX	YYYYYYY

1-3. デバイス情報

本システムに使用する機器のデバイス情報とライセンス情報を以下に示す。

項目	アクティブ機	スタンバイ機
ASA バージョン	8.2.3	8.2.3
ASDM バージョン	6.3.4	6.3.4
ファイアーウォールモード	Routed	Routed
コンテキストモード	Single	Single
ライセンス	VPN Plus	VPN Plus
最大コンテキスト数	2	2
最大 VLAN 数	150	150
最大物理接続数	Unlimited	Unlimited
Failover 機能	Active/Active	Active/Active
IPsec VPN ピア数	750	750
SSL VPN ピア数	2	2
VPN DES Encryotion	Enable	Enable
VPN 3DES and AES Encryotion	Enable	Enable
AnyConnect Mobile	Disable	Disable

ネットワーク設計

1-3-1. インターフェイス設定

本システムの各インターフェイスのネットワーク設定を以下に示す。

■FW1（アクティブ機）

Interface	Name	Enabled	Security Level	IP Address	Redundant	Management Only	MTU	Speed	Duplex
GigabitEthernet0/0	outside	Yes	0	Use PPPoE	No	No	1500	Auto	Auto
GigabitEthernet0/1	inside	Yes	100	172.16.10.10/24	No	No	1500	Auto	Auto
GigabitEthernet0/2	DMZ	Yes	50	172.16.20.20/24	No	No	1500	Auto	Auto
GigabitEthernet0/3	-	No	-	-	No	No	-	-	-
Management0/0	mgmt	No	100	192.168.10.10	No	No	1500	Auto	Auto

■FW2（スタンバイ機）

Interface	Name	Enabled	Security Level	IP Address	Redundant	Management Only	MTU	Speed	Duplex
GigabitEthernet0/0	outside	Yes	0	Use PPPoE	No	No	1500	Auto	Auto
GigabitEthernet0/1	inside	Yes	100	172.16.10.11/24	No	No	1500	Auto	Auto
GigabitEthernet0/2	DMZ	Yes	50	172.16.20.21/24	No	No	1500	Auto	Auto
GigabitEthernet0/3	-	No	-	-	No	No	-	-	-
Management0/0	mgmt	No	100	192.168.10.11	No	No	1500	Auto	Auto

■PPPoE 設定

項目	IP Address
Group Name	PPPoE-Group
PPPoE Username	ABC123
PPPoE Password	chap
PPP Authentication	**********
Store username and password in local flash	Enabled

1-3-2. ルーティング設定

1-3-3. 高可用性設計

2. ファイアーウォール設計

2-1. ファイアーウォール オブジェクト設計

2-1-1. ネットワークオブジェクト

・ ネットワークオブジェクトについて

ネットワークオブジェクトは、ホストおよびネットワークの IP アドレスを事前に定義して、以降の設定を効率よく行うためのものである。アクセスルールや AAA ルールなどのセキュリティポリシーを設定すると、手動で入力する代わりに事前定義済みのアドレスを選択可能となる。さらに、オブジェクトの定義を変更した場合、変更内容は自動的にそのオブジェクトを使用するすべてのルールに継承される。

ネットワークオブジェクトの設定を以下に示す。

Name	IP Address	備考
outside-network	-	PPPoE 接続
inside1-network	172.＊＊.＊＊.0/24	
inside2-network	172.＊＊.＊＊.0/24	

2-1-2. サービスグループ設定

・ サービスグループについて

サービスグループは、指定したグループに複数のサービスを関連付けるものである。 1 つのグループに任意のタイプのプロトコルとサービス（ポートナンバー）を指定し、アクセスルール作成時に複数のサービスを定義することが可能である。

サービスグループの設定を以下に示す。

Service	Protocol	備考
RDP	TCP/3389	-

2-2. ファイアーウォールポリシー設計

以下にネットワークアクセス制御ポリシーの設定を示す。

・inside1-network/24(172.＊＊.＊＊.0/24)から inside2-network/24(172.＊＊.＊＊.0/24)と outside-network(インターネット)へのアクセスを許可する。

・inside2-network/24(172.＊＊.＊＊.0/24)から iinside1-network/24(172.＊＊.＊＊.0/24)と outside-network(インターネット)へのアクセスを許可する。

・outside-network からは全てのアクセスを拒否する。ただしリモートアクセスサービスへの接続はこのポリシーから除外される。

inside_access_in　<inside ネットワークへのアクセス>

#	Enabled	Source <送信元>	Destination <送信先>	Service	Protocol	Action	Logging
1	On	inside1-network/24	any	ip	-	Permit	Default
2	On	any	any	ip	-	Deny	-

DMZ_access_in　<DMZ ネットワークへのアクセス>

#	Enabled	Source <送信元>	Destination <送信先>	Service	Protocol	Action	Logging
1	On	inside2-network/24	any	ip	-	Permit	Default
2	On	any	any	ip	-	Deny	-

outside_access_in　<outside ネットワークへのアクセス>

#	Enabled	Source <送信元>	Destination <送信先>	Service	Protocol	Action	Logging
1※	On	any	any	ip	-	Deny	Default
2	On	any	any	ip	-	Deny	-

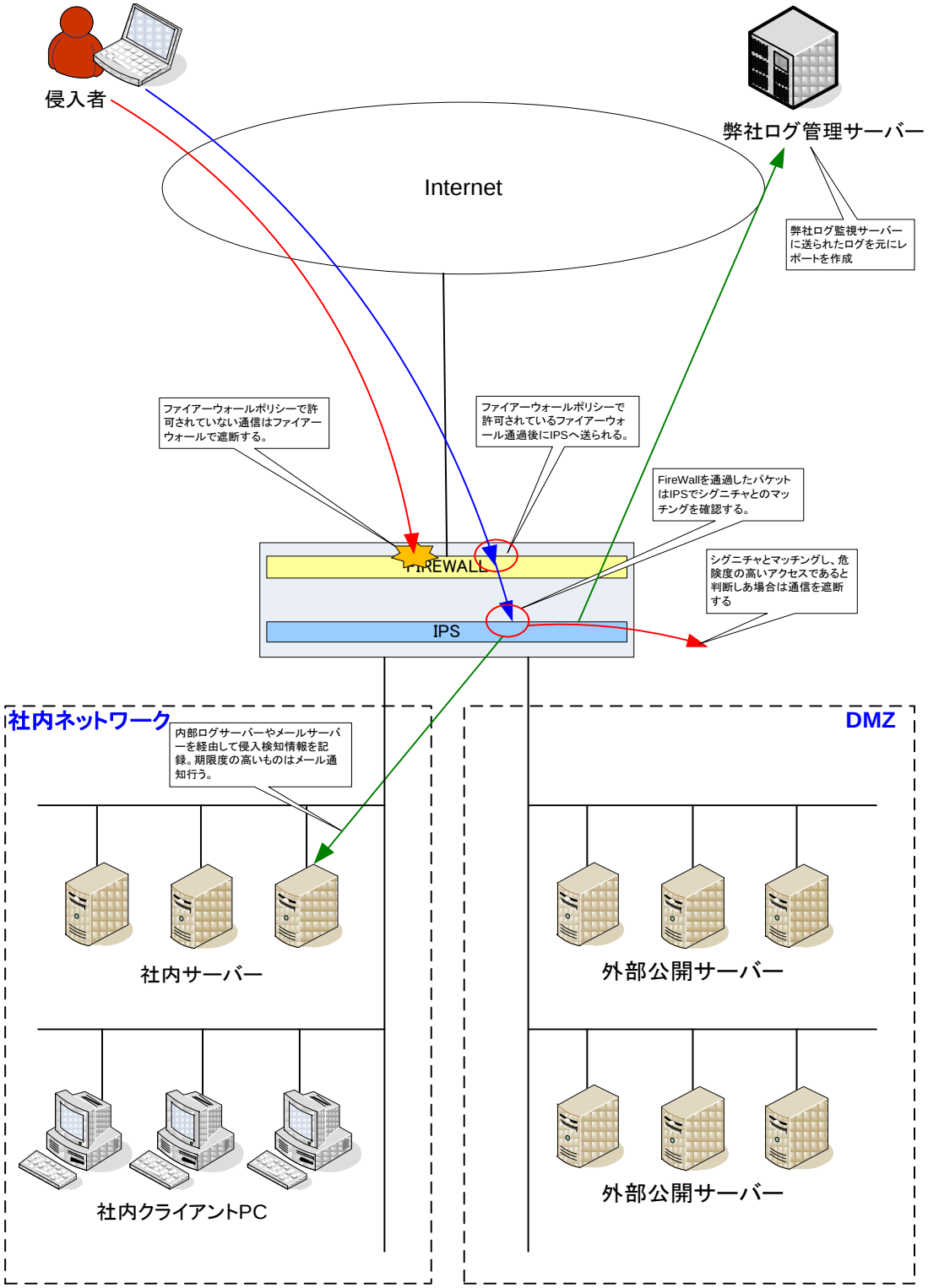
※Deny ログ取得用の Access Rule

3. 侵入検知設計

3-1. 侵入検知動作設計

3-1-1. 侵入検知動作概略図 と動作モード

本システムの侵入検知動作の概略図を以下に示す。

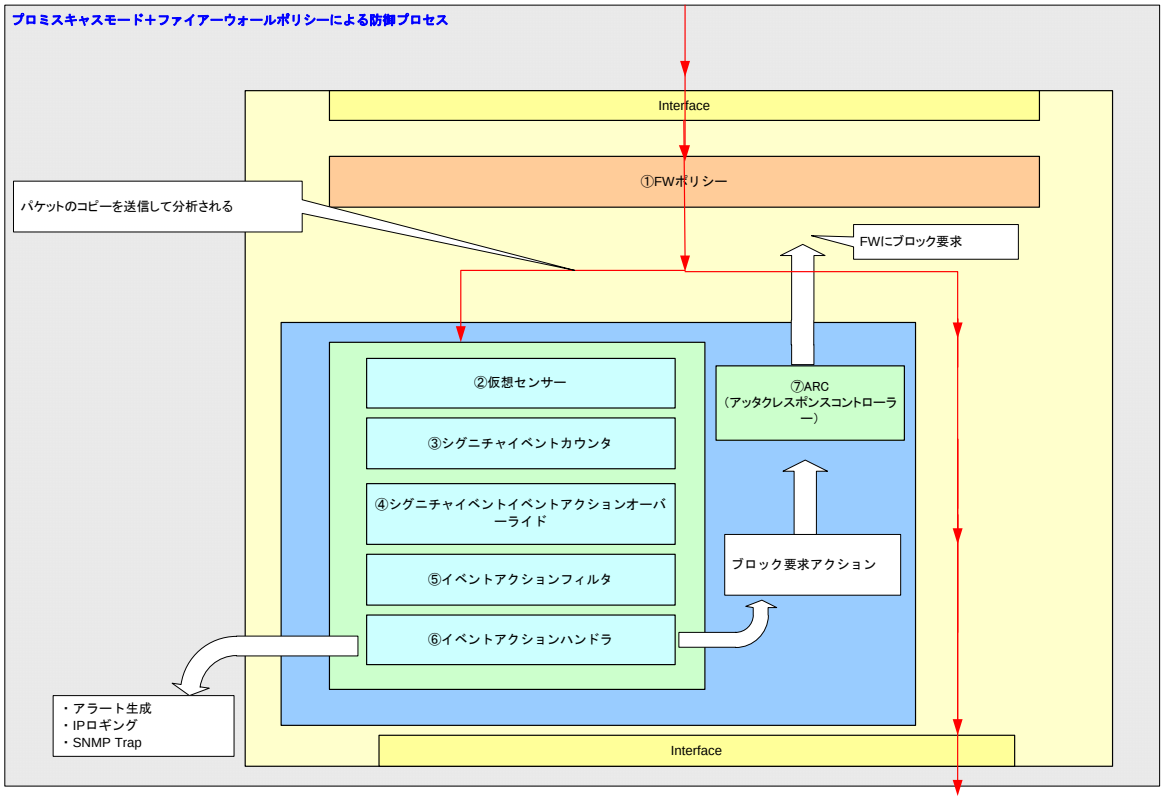


3-2. シグニチャ設計

3-3. ブロッキング設計

3-3-1. ブロッキング動作設計

本システムのブロッキングには Attack Response Controller（以下 ARC）の機能を使って、ブロッキングデバイスにブロッキング要求を行う。本システムのブロッキングデバイスは ASA5520 となり、Firewall 機能のアクセス制御によって攻撃元ホストおよびネットワークからの不正なアクセスをブロックする。ARC はブロック時間を監視し、その時間が満了するとブロックを解除する。以下はブロッキング時のプロセスを示した図である。



ASA5520によるファイアーウォール機能	
機能	動作内容
①FWポリシー	FWポリシーでの接続許可

AIP-SSM20（Cisco IPS）による侵入検知機能	
機能	動作内容
②仮想センサー	各シグニチャ定義での検知 検知したシグニチャのイベント発生
③シグニチャイベントカウンタ （各シグニチャ個別のイベントアクション）	イベントカウンタの値に達すると各シグニチャで設定されたイベントを追加
④シグニチャイベントイベントアクションオーバーライド （RRに基づいてアクションを追加する機能）	RiskRateに基づくアクションを追加
⑤イベントアクションフィルタ （シグニチャID、アドレス、ポート、RRなどに基づいてアクションを削除する機能）	シグニチャID、アドレス、ポート、RRなどに基づいてアクションを削除
⑥イベントアクションハンドラ （イベントアクションを実行する機能）	アラート生成 ブロック（inlineモード） SNMP Trap ブロッキング要求
⑦ARC （アタックレスポンスコントローラー）	ブロキングデバイス（ASA5520）へブロッキング要求を行う

①FWポリシー	FWポリシーでの接続拒否

4. 運用管理設計

株式会社レップワン

SAMPLE

株式会社 XXXX 御中

ファイアーウォール・侵入検知システム
運用手順書

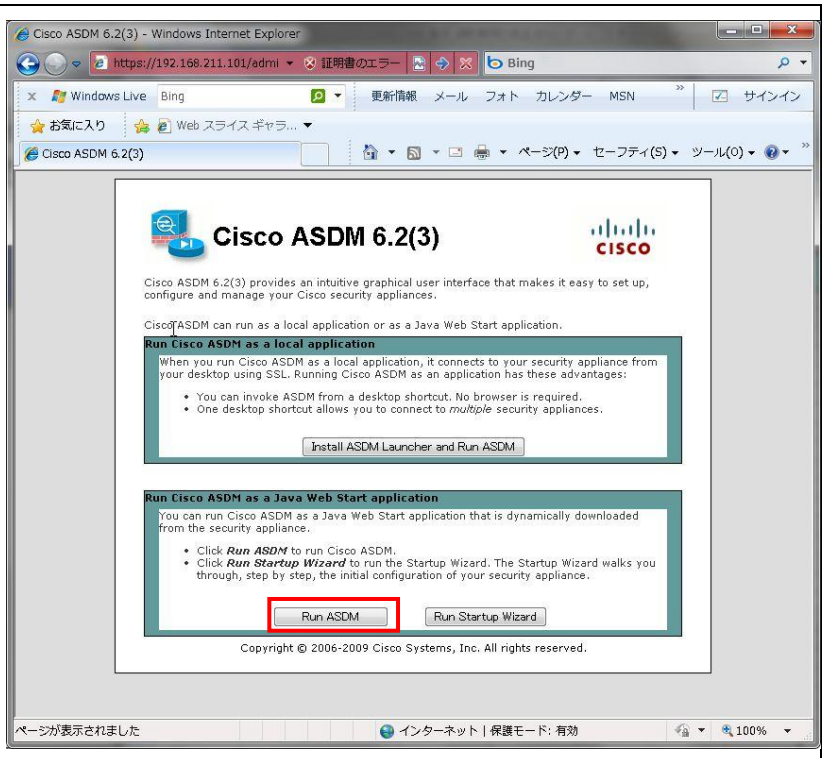
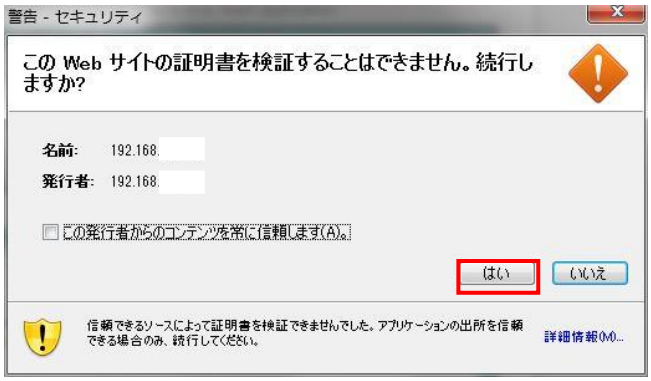
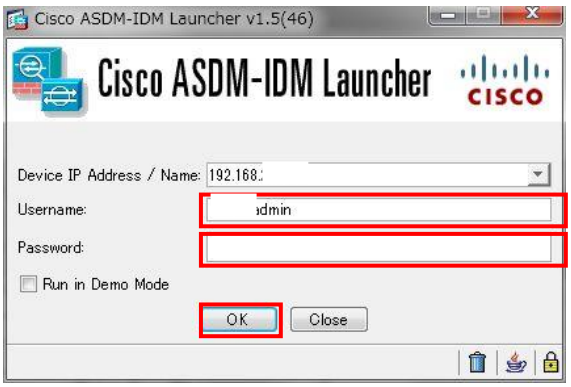
作成者：株式会社レップワン

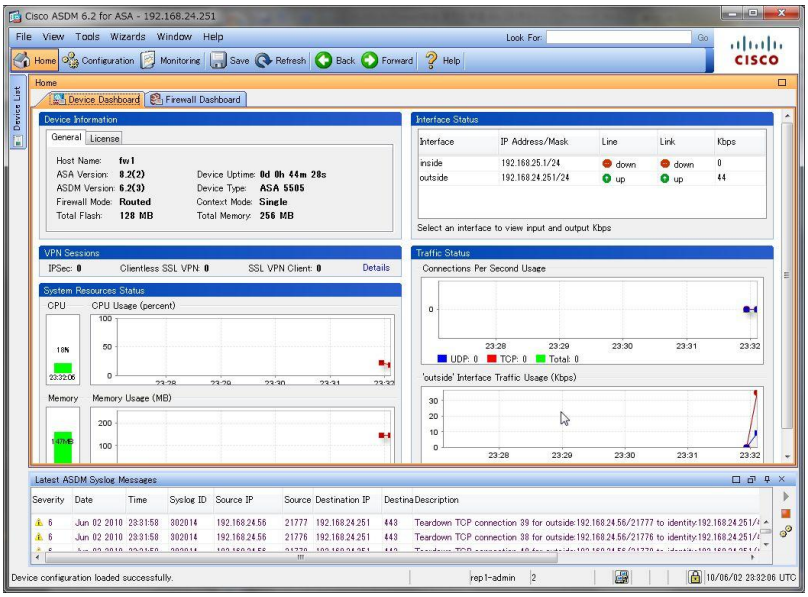
作成日時：2011/XX/XX

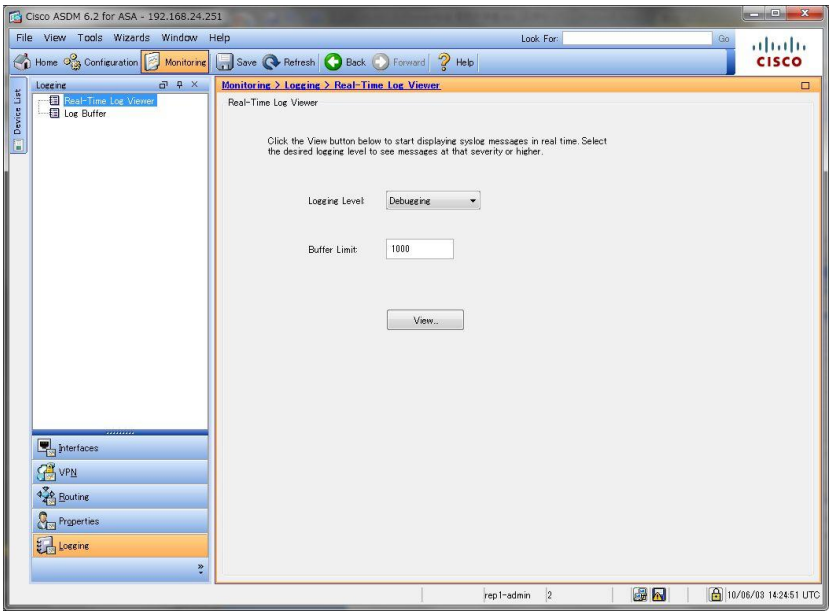
目次

1. 管理 GUI：ASDM へのログイン手順

ASA5520をGUIで設定・操作するためのASDMを起動・ログインする手順です。

1	Web ブラウザを立ち上げ https://XXXXXX へアクセスする。 ページが表示されたら Run ASDM ボタンをクリックする。	
2	証明書の確認画面が表示されるので「はい」を選ぶ。	
3	ログイン情報入力のポップアップが表示されるので Username：XXXXXX Password：別途資料記載 を入力し、OK ボタンを押す。	

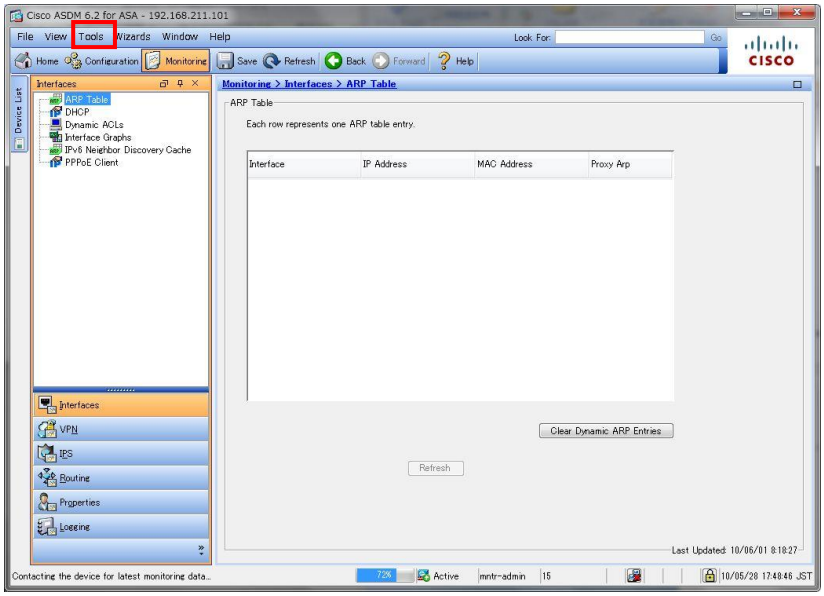
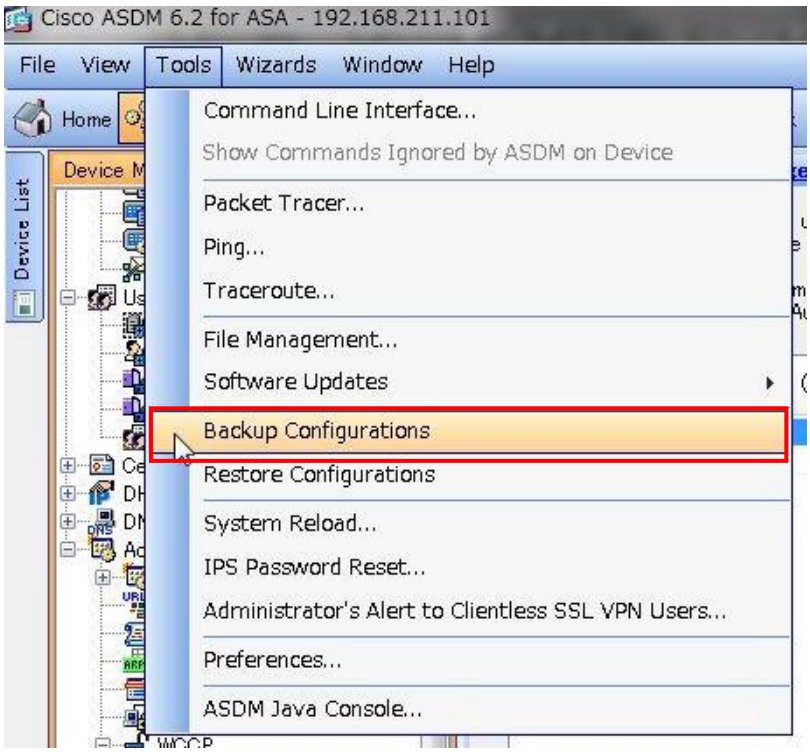
4	ログイン出来ると各種設定・操作を ASDM で可能となる。	

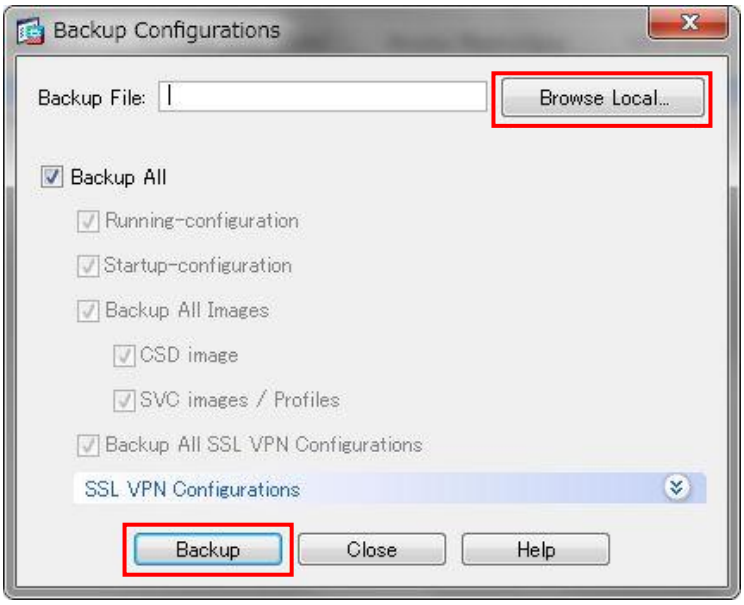
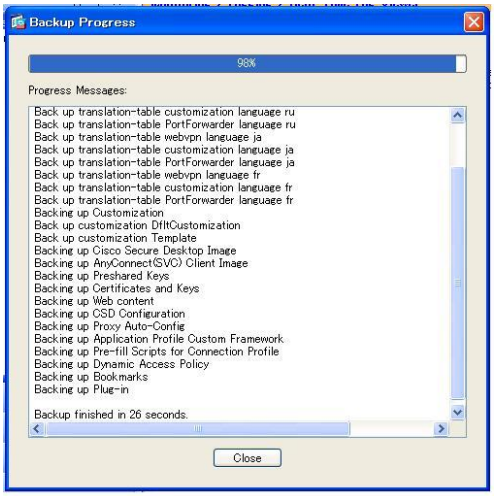
5	Real-Time Log Viewer を選択した場合、確認したいログレベルを Logging Level から選択し、Buffer Limit 欄に最大表示数を入力して（デフォルトは 1000 件）View ボタンを押す。	

設定バックアップ・リストア手順

1. 設定バックアップ

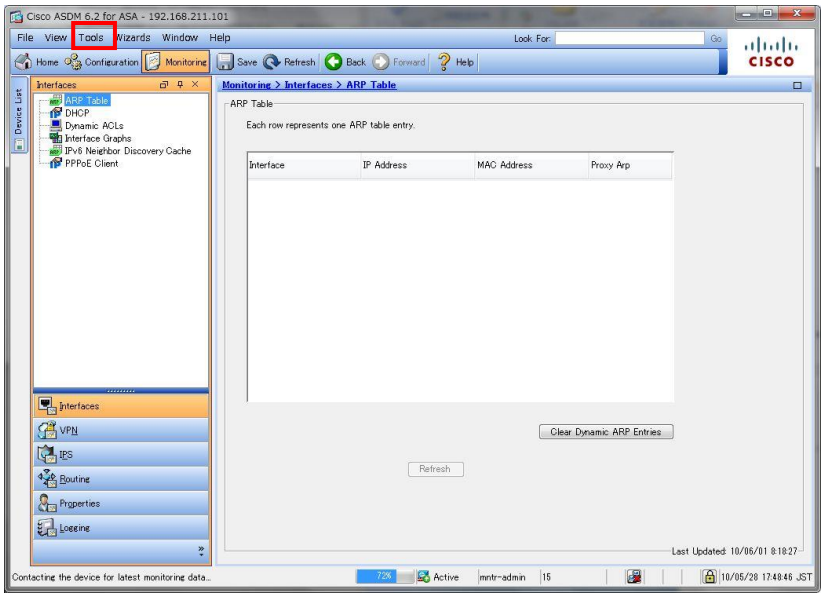
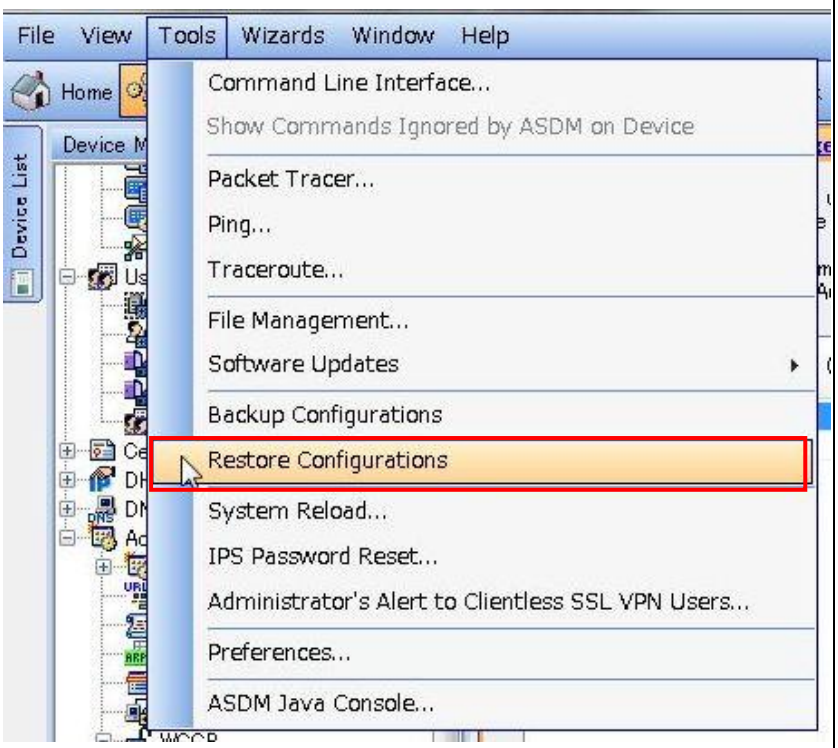
現在稼働中の設定のバックアップを取得する手順です。

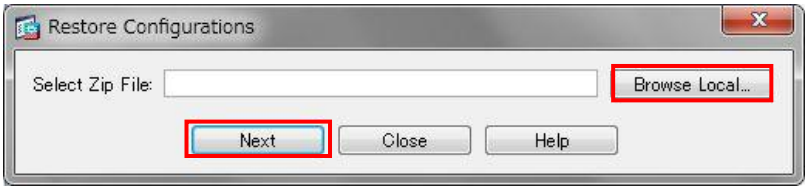
項番	手順	図
1	ASDM を起動後上部ツールバーで「Tools」を選択する。	
2	ドロップダウンメニューが表示されるので Backup Configurations を選択する。	

3	ポップアップ画面が表示されるので、Browse Local ボタンを押して保存先とファイル名を指定する。 下部の Backup ボタンを押すとバックアップが開始される。	
4	バックの進行状況が表示される。	
5	バックアップのレポートが表示されたら OK ボタンを押してポップアップを閉じる。 その後、指定した保存場所に設定ファイルが ZIP ファイルとして保存されている事を確認する。	

2. 設定リストア

障害や設定変更で動作に問題があった場合に以前保存したバックアップファイルから設定を戻す手順です。

項番	手順	図
1	ASDM を起動後上部ツールバーで「Tools」を選択する。	
2	ドロップダウンメニューが表示されるのでRestore Configurations を選択する。	

3	ポップアップが表示されるので Browse Local ボタンを押して設定ファイル保存先から指定し、Next ボタンで次へ進む。	
4	リストアを行いたい設定ファイルにチェックして Restore ボタンを押すとリストアが開始される。