HITACHI
Inspire the Next

ファイアウォールログ解析ソフトウェア

FIREWALLstaff

取扱説明書（ファイアウォール設定編）

株式会社 日立ソリューションズ

■ 対象製品

FIREWALLstaff 02-08

■ 輸出時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。

なお，ご不明な場合は，弊社または弊社販売店の担当窓口へお問い合わせください。

■ 商標類

- Windows，Windows Server は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Microsoft は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。
- NETSCREEN，JUNIPER NETWORKS はそれぞれジュニパーネットワークス社の登録商標です。
- FORTIGATE はフォーティネット社の登録商標です。
- PALO ALTO NETWORKS はパロアルトネットワークス社の商標です。
- チェック・ポイント，VPN-1 UTM は，Check Point Software Technologies Ltd.およびその関連会社の商標，又は登録商標です。
- IPCOM は，富士通株式会社の登録商標です。
- Cisco，Cisco Systems，および Cisco Systems ロゴは，米国 Cisco Systems，Inc. の米国および他の国々における登録商標です。
- FIREWALLstaff は，株式会社日立ソリューションズの登録商標です。
- その他，本マニュアル記載の会社名，製品名は，それぞれの会社の商号，登録商標または商品名称です。

■ 発行

2021 年 12 月

はじめに

このマニュアルは，FIREWALLstaff でレポートを作成するために必要な，ファイアウォールの設定について説明したものです。

■ 対象読者

FIREWALLstaff を運用，管理するシステム管理者を対象としています。

このマニュアルの記述は，次の事項を前提にしています。

- Windows の基本操作を習得している。
- コンピュータの管理者として必要な知識がある。
- ネットワークに関する基本的な知識がある。
- セキュリティに関する基本的な知識がある。
- ファイアウォールの設定変更ができる。

■ このマニュアルでの表記

このマニュアルでは製品名称について次のように表記しています。ただし，それぞれの製品についての表記が必要な場合はそのまま表記しています。

製品名称	表記
Juniper NetScreen	NetScreen
Juniper SSG	SSG
Juniper SRX	SRX
Fortinet FortiGate	FortiGate
Palo Alto Networks PA	Palo Alto
CheckPoint Software Blade	CheckPoint
IPCOM EX IN/SC	IPCOM
Cisco ASA	Cisco

■ 画面操作説明で使う表記

画面操作説明で使う表記を次に示します。

記号	意味
［ ］	ボタンやテキストボックスなど，画面に表示されている要素を示します。
［ ］－［ ］	画面に表示されるメニューやアイコンなどを選択する操作を示します。

■ 常用漢字以外の漢字の使用について

このマニュアルでは常用漢字を使用することを基本としていますが，次に示す用語については常用漢字以外の漢字を使用しています。

鍵（かぎ）　個所（かしょ）　必須（ひっす）

■ MB（メガバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイトです。

目次

1 Juniper NetScreen/SSG シリーズ

1.1 Juniper NetScreen/SSG の設定

1.1.1 サポート機種，OS バージョン

Juniper NetScreen シリーズ，Juniper SSG シリーズのファイアウォールで，ScreenOS が ScreenOS5.4～ScreenOS6.3 のいずれかであるファイアウォール。

1.1.2 設定手順

NetScreen/SSG のログを解析してレポートするために必要な，NetScreen/SSG の設定について説明します。GUI で設定できることについては GUI を用いた設定手順を説明しますので，CUI を用いて設定する場合は，NetScreen/SSG のマニュアルをご参照ください。

なお，ScreenOS6.3 における設定手順を説明しておりますので，他の ScreenOS の場合は，NetScreen/SSG のマニュアルなどもあわせてご参照ください。

(1) Syslog 送信の設定

NetScreen/SSG から，ログ（Syslog）を送信する設定を行います。

[Configuration]－[Report Settings]－[Syslog]を選択します（図 1 参照）。

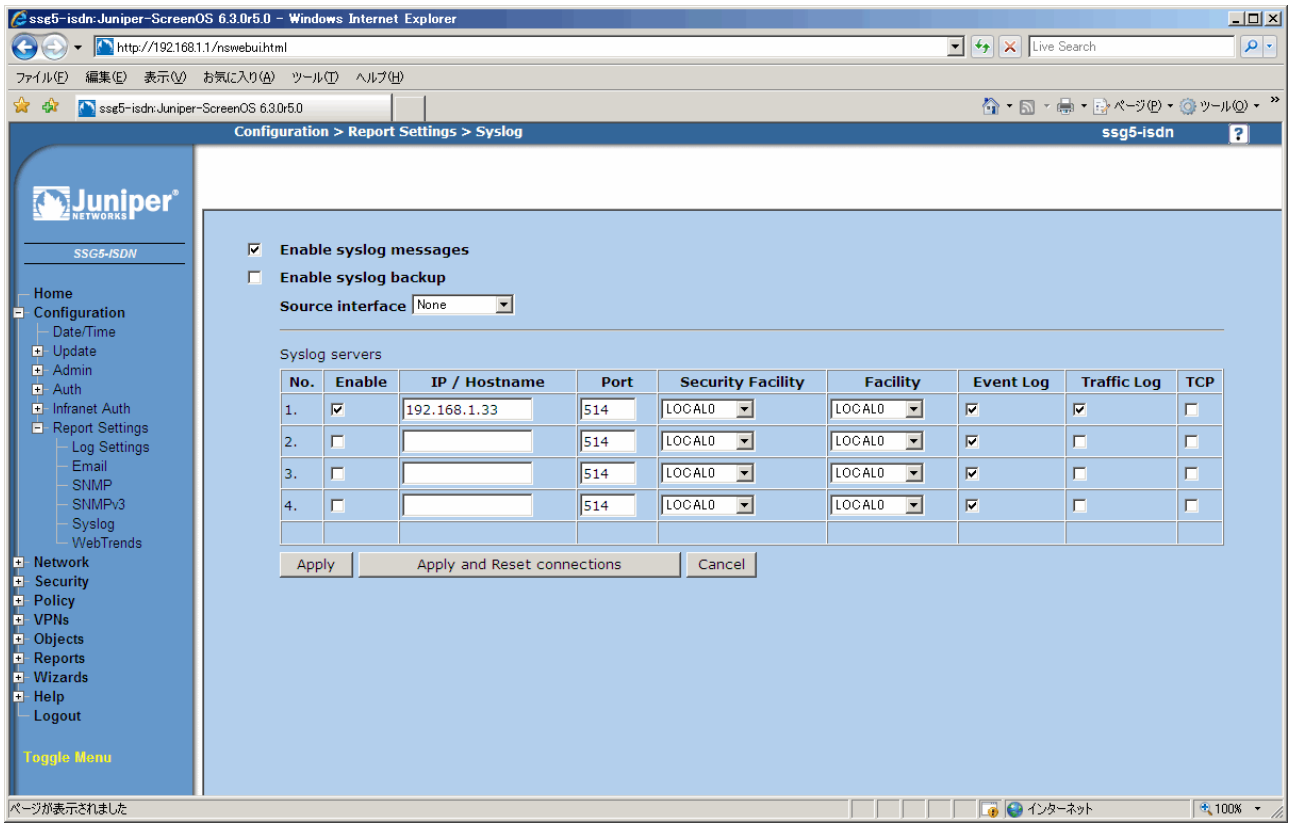


図 1 [Syslog]ウィンドウ

- [Enable syslog messages]チェックボックスを選択します。
- Syslog servers 項目で，[Enable]チェックボックスを選択します。
- [IP/Hostname]に，Syslog を受信するマシン（例，FIREWALLstaff AE Server をインストールしたマシン）の IP アドレスを指定します。
- [Port]に，Syslog を受信するマシン（例，FIREWALLstaff AE Server をインストールしたマシン）での Syslog 待ちうけポート番号（通常は 514）を指定します。
- [Event Log][Traffic Log]チェックボックスを選択します。
- TCP でログを送信する場合は[TCP]チェックボックスを選択します。
- 最後に，[Apply]をクリックします。

[Configuration]－[Report Settings]－[Log Settings]を選択します（図 2 参照）。

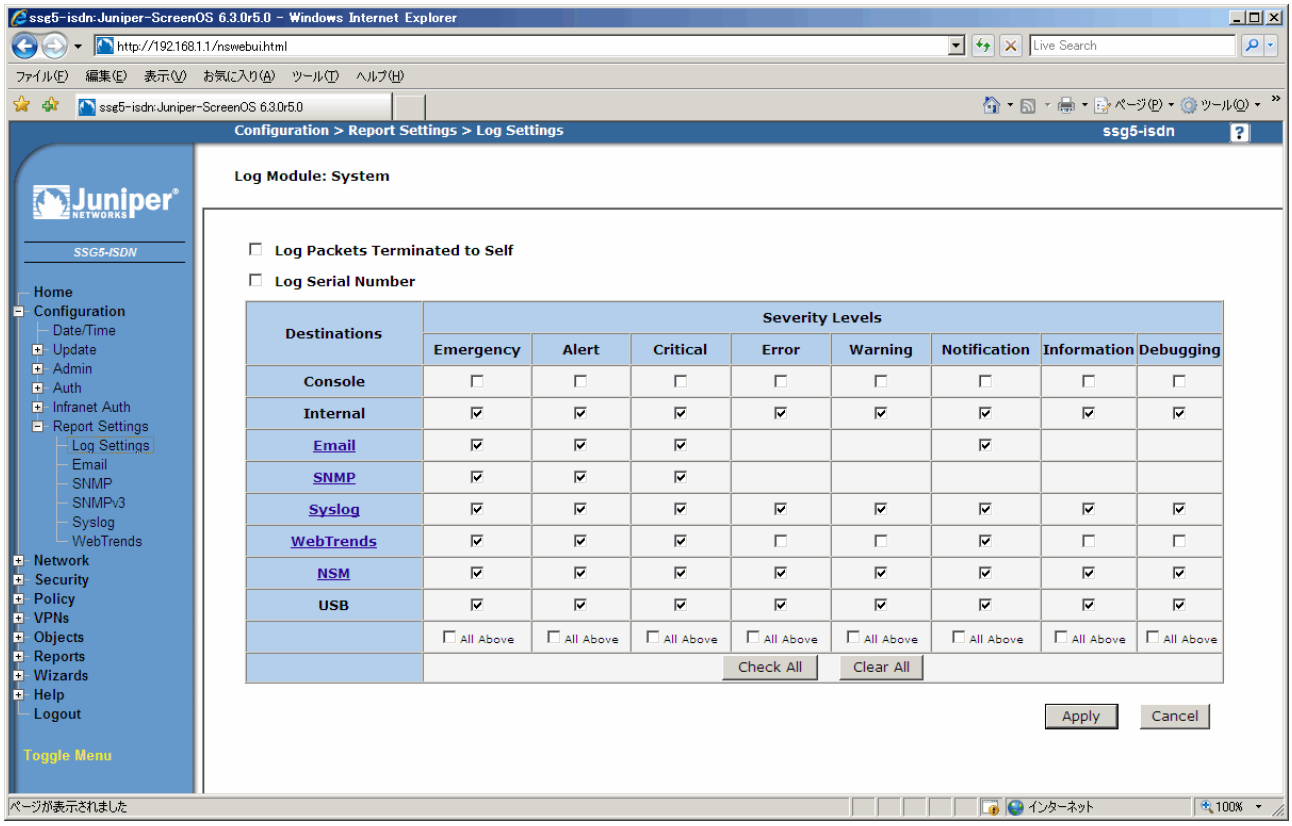


図 2 [Log Settings]ウィンドウ

- [Syslog]の[Severity Levels]について，表 1.1-1 を参考に，適切な[Severity Levels]を指定します。
- 最後に，[Apply]をクリックします。

表 1.1-1 ログレベル

ログレベル		FIREWALLstaff に関連するログ
0	Emergency	攻撃
1	Alert	攻撃
2	Critical	攻撃
3	Error	攻撃
4	Warning	攻撃，ウイルス，スパム，URL フィルタ
5	Notification	攻撃，トラフィック
6	Information	攻撃

(2) ポリシ毎のログ出力の設定

すでに設定されている NetScreen/SSG の各ポリシに，ログを出力する設定を行います。

[Policy]－[Policies]を選択します（図 3 参照）。

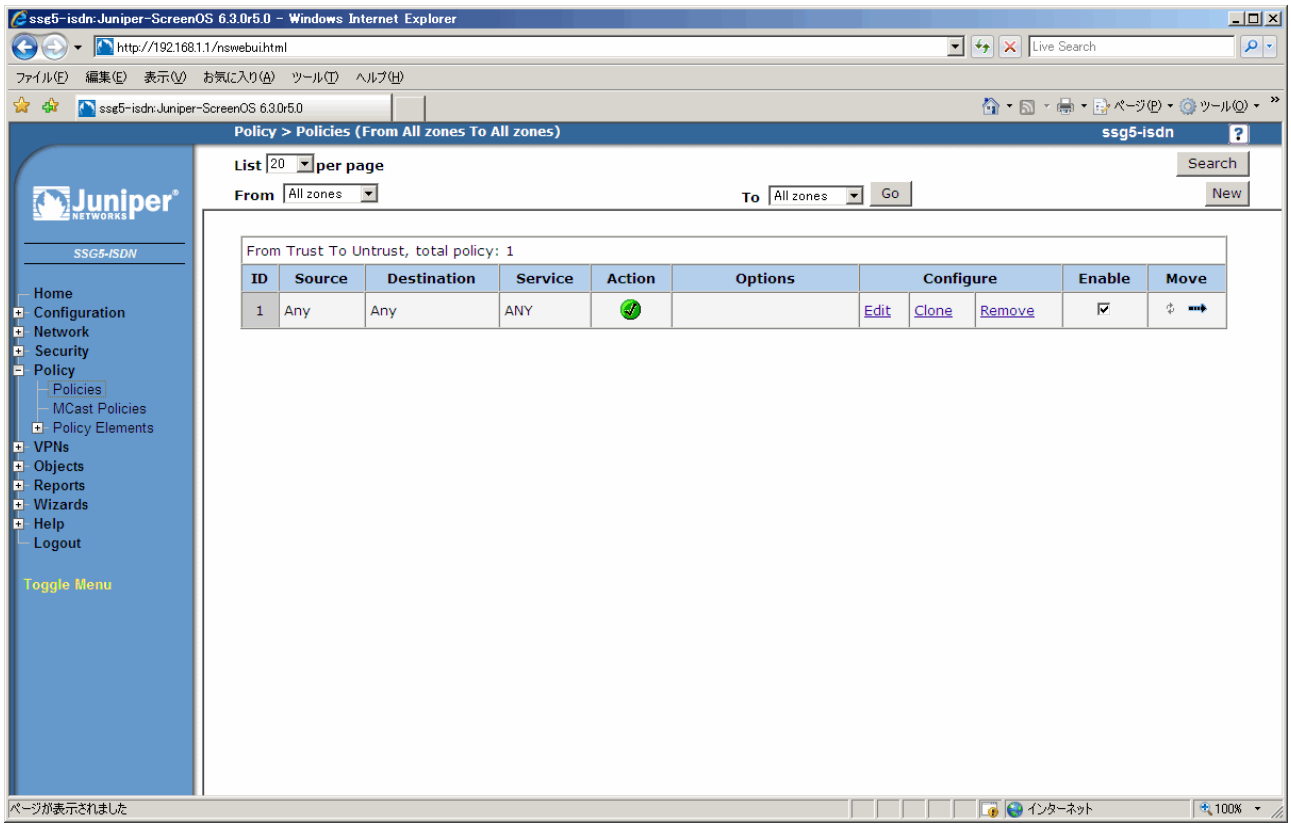


図 3 [Policies]ウィンドウ

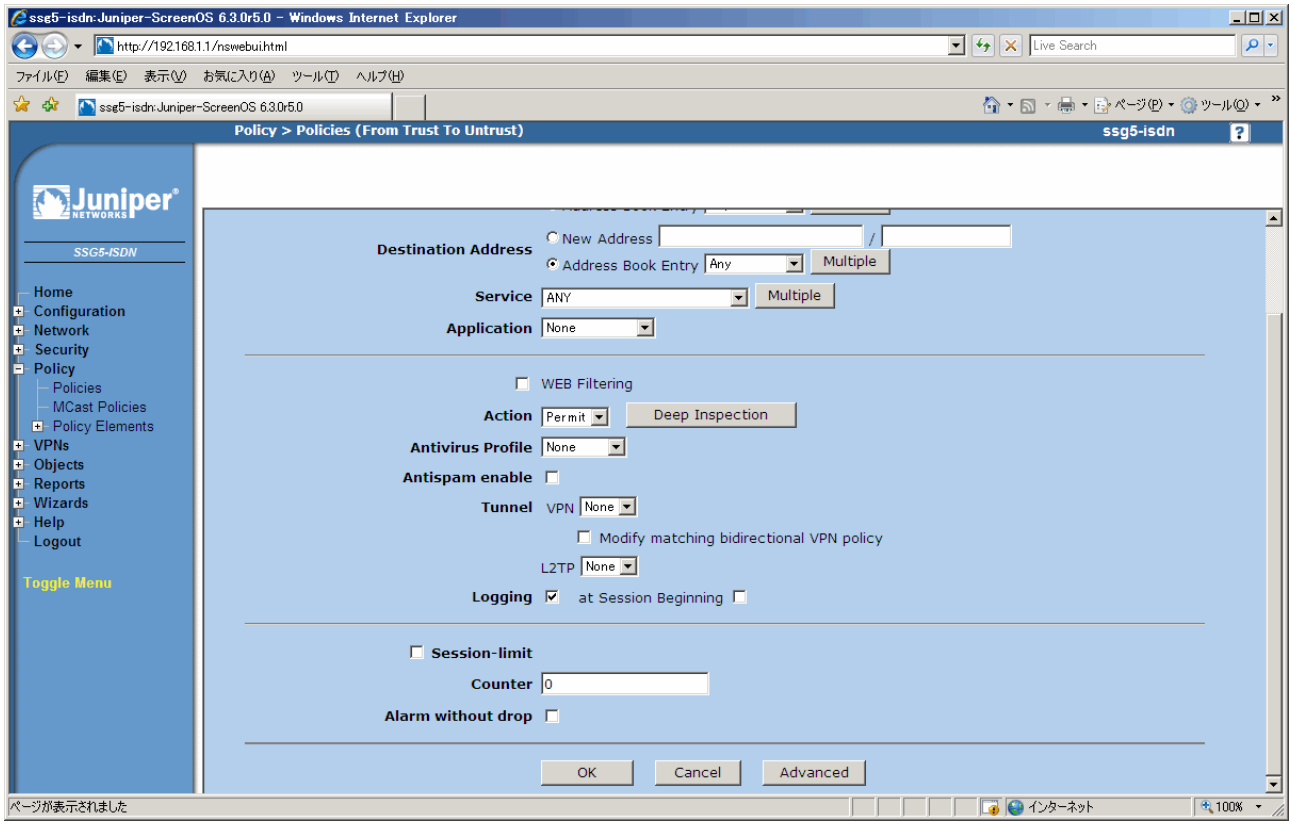


図 4 [Policies]の編集ウィンドウ

- ログを出力するポリシの[Configure]項目で，[Edit]をクリックします（クリックしたウィンドウを図 4 に示します）。
- [Logging]チェックボックスを選択します。
- 最後に，[OK]をクリックします。

2 Fortinet FortiGate シリーズ

2.1 Fortinet FortiGate シリーズの設定

2.1.1 サポート機種，OS バージョン

FortiGate シリーズのファイアウォールで，FortiOS が FortiOS4.0MR3～FortiOS 6.4.6 のいずれかであるファイアウォール。

2.1.2 設定手順

FortiGate のログを解析してレポートするために必要な，FortiGate の設定について説明します。GUI で設定できることについては GUI を用いた設定手順を説明しますので，CUI を用いて設定する場合は，FortiGate のマニュアルをご参照ください。

なお，FortiOS5.0 における設定手順を説明しておりますので，他の FortiOS の場合は，FortiGate のマニュアルなどもあわせてご参照ください。

(1) Syslog 送信の設定

FortiGate から，ログ（Syslog）を送信する設定を行います。

FortiGate にログインし，次のコマンドを実行します。

```
config log syslogd setting
set status enable
set server Syslog を受信するマシンの IP アドレス
end
```

例

```
# config log syslogd setting↵
(setting) # set status enable↵
(setting) # set server 192.168.1.110↵
(setting) # end↵
```

(2) ポリシ毎のログ書き出しの設定

すでに設定されている FortiGate の各ポリシに，ログを出力する設定を行います。

[ポリシー]－[ポリシー]－[ポリシー]を選択します（図 5 参照）。

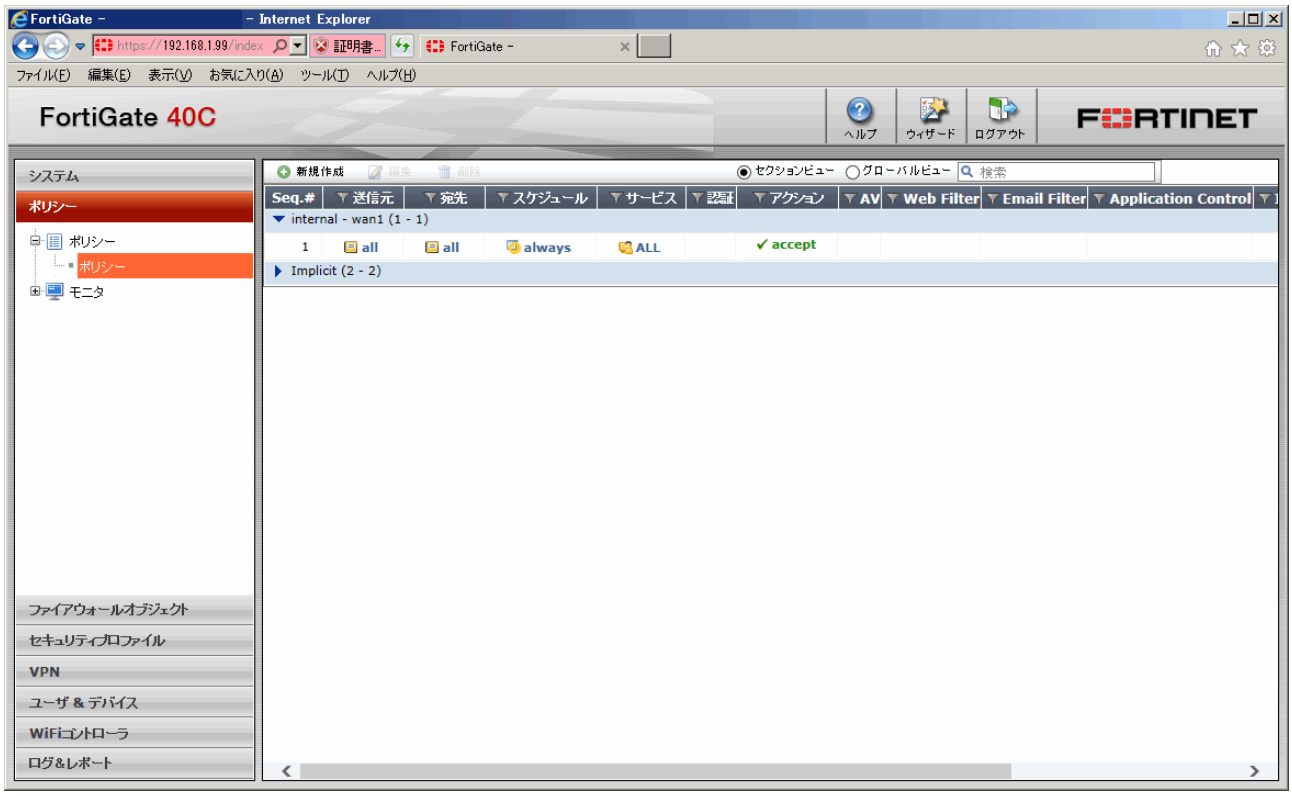


図 5 [ポリシー]ウィンドウ

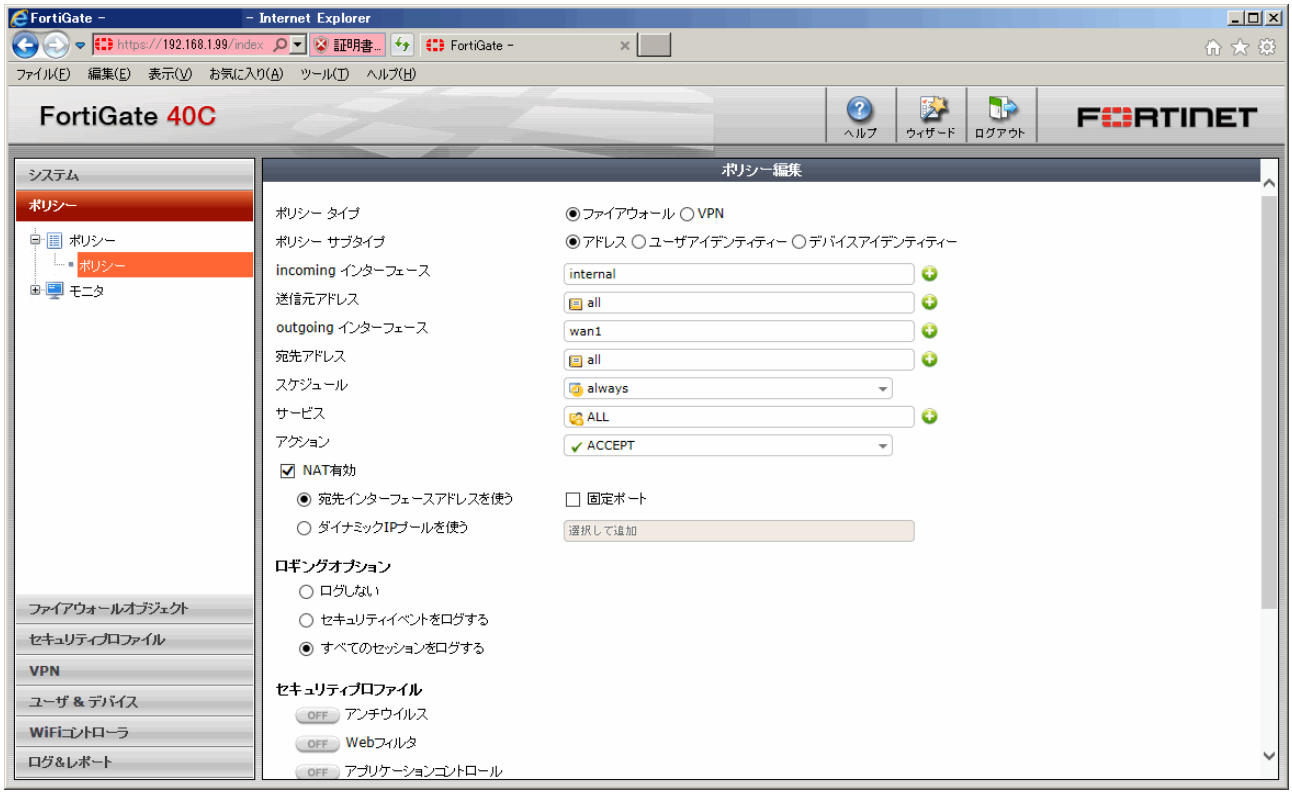


図 6 [ポリシー]の編集ウィンドウ

- ログを出力するポリシの[編集]をクリックします（クリックしたウィンドウを図 6 に示します）。
- [すべてのセッションをログする]を選択します。
- 最後に，[OK]をクリックします。

(3) その他のログ書き出しの設定

必要に応じて，UTM 関連のログを出力する設定を行います。

- アンチウイルス
- Web フィルタ
- アプリケーションコントロール
- 侵入防御
- Email フィルタ

なお，「URL フィルタリング」のレポートは，「FortiGuard カテゴリ」のログのみをレポート対象とします。

3 Palo Alto PA シリーズ

3.1 Palo Alto PA シリーズの設定

3.1.1 サポート機種，OS バージョン

Palo Alto PA シリーズのファイアウォールで，OS が PANOS3.1.x～PANOS9.1.x のいずれかであるファイアウォール。

3.1.2 設定手順

Palo Alto のログを解析してレポートするために必要な，Palo Alto の設定について説明します。GUI で設定できることについては GUI を用いた設定手順を説明しますので，CUI を用いて設定する場合は，Palo Alto のマニュアルをご参照ください。

なお，PANOS5.0.4 における設定手順を説明しておりますので，他の PANOS の場合は，Palo Alto のマニュアルなどもあわせてご覧ください。

(1) Syslog 送信の設定

Palo Alto から，ログ（Syslog）を送信する設定を行います。

[Device]-[セットアップ]を選択し，[サービス]タブをクリックします（図 7 参照）。

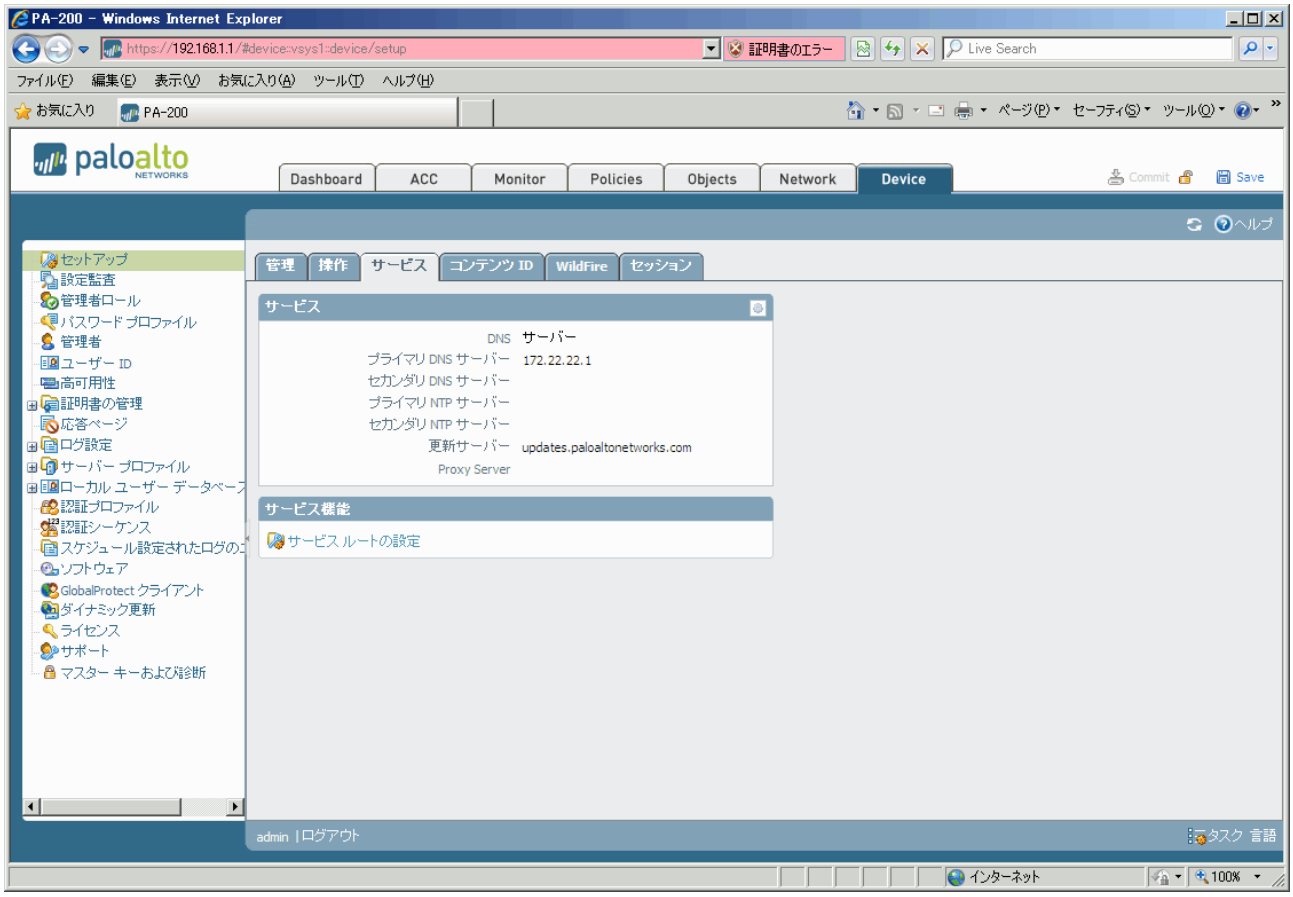


図 7 [セットアップ]ウィンドウ

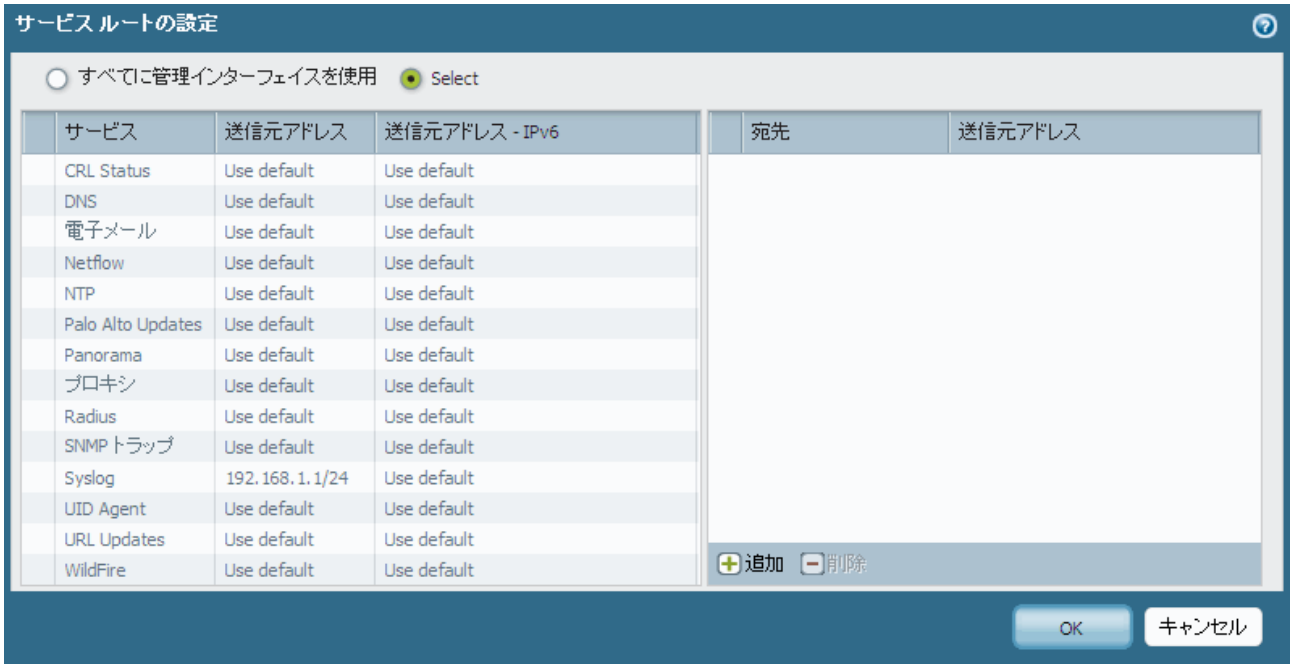


図 8 [サービスルートの設定]ウィンドウ

- [サービスルートの設定]をクリックします（クリックして開かれたウィンドウを図 8 に示します）。
- [Select]を選択し，[Syslog]の[送信元アドレス]ドロップダウンリストから，適切な Syslog 送信元を選択し，[OK]をクリックします。

[Device]-[サーバープロファイル]-[Syslog]を選択します（図 9 参照）。

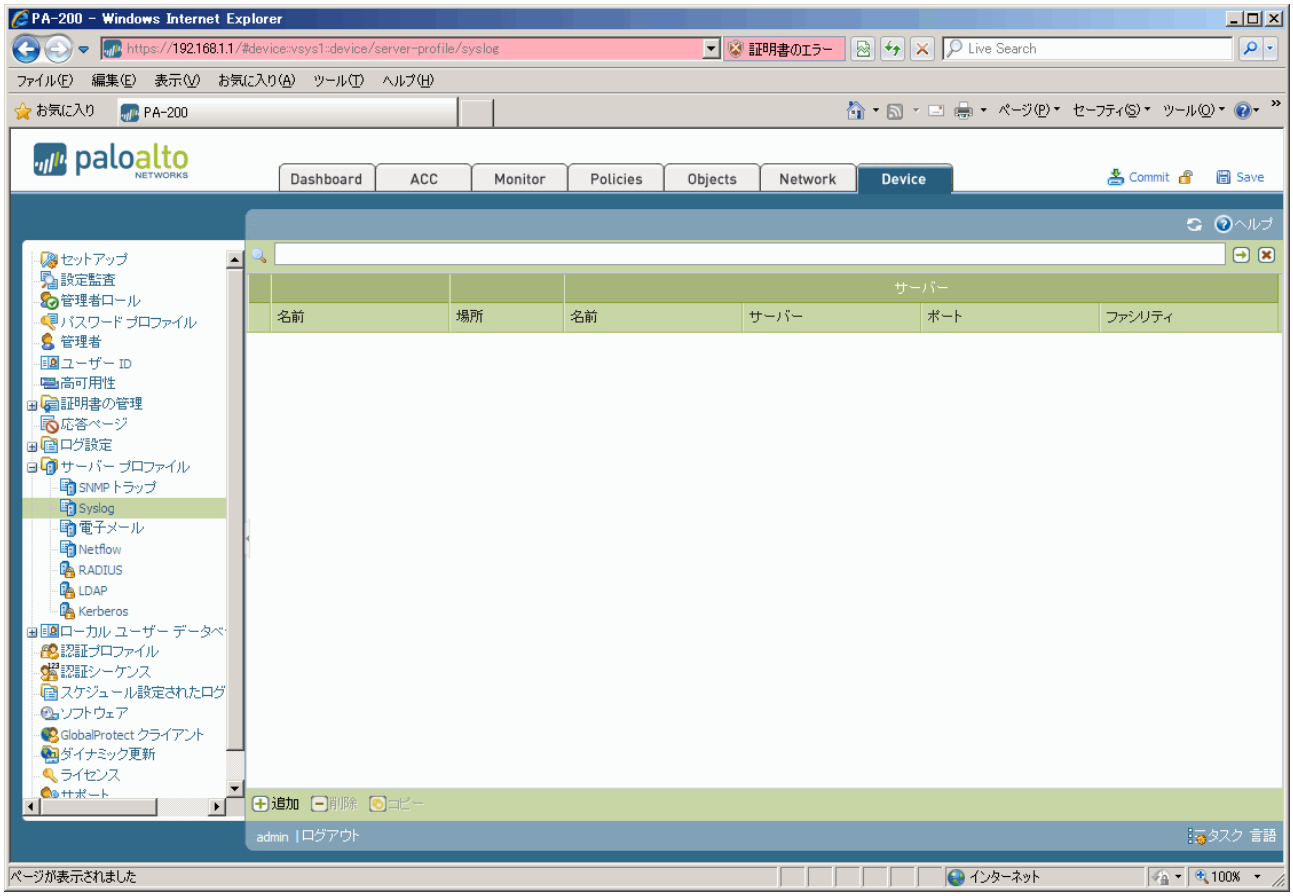


図 9 [Syslog]ウィンドウ

図 10 [Syslog サーバープロファイル]ウィンドウ

- [追加]ボタンをクリックします(クリックして開かれたウィンドウを図 10 に示します)。
- [名前]を指定します。**ここで指定した名称を「名称１」とします**。
- [サーバー]タブをクリックして，[追加]ボタンをクリックします。
- [サーバー]-[名前]を指定します。
- [サーバー]-[Syslog サーバー]に，FIREWALLstaff AE Server をインストールしたマシンの IP アドレスを指定します。
- [サーバー]-[転送]に，UDP または TCP のいずれかを指定します。
- [サーバー]-[ポート]に，FIREWALLstaff AE Server での Syslog 待ちうけポート番号（通常は 514）を指定します。
- [サーバー]-[ポート]は，BSD を指定します。
- [サーバー]-[ファシリティ]は，LOG_USER を指定します。
- 最後に，[OK]をクリックします。

注　意

[カスタムログフォーマット]タブの内容は,初期値のままとしてください。変更した場合,FIREWALLstaff でログの解析ができなくなります。

[Objects]-[ログ転送]を選択します（図 11 参照）。

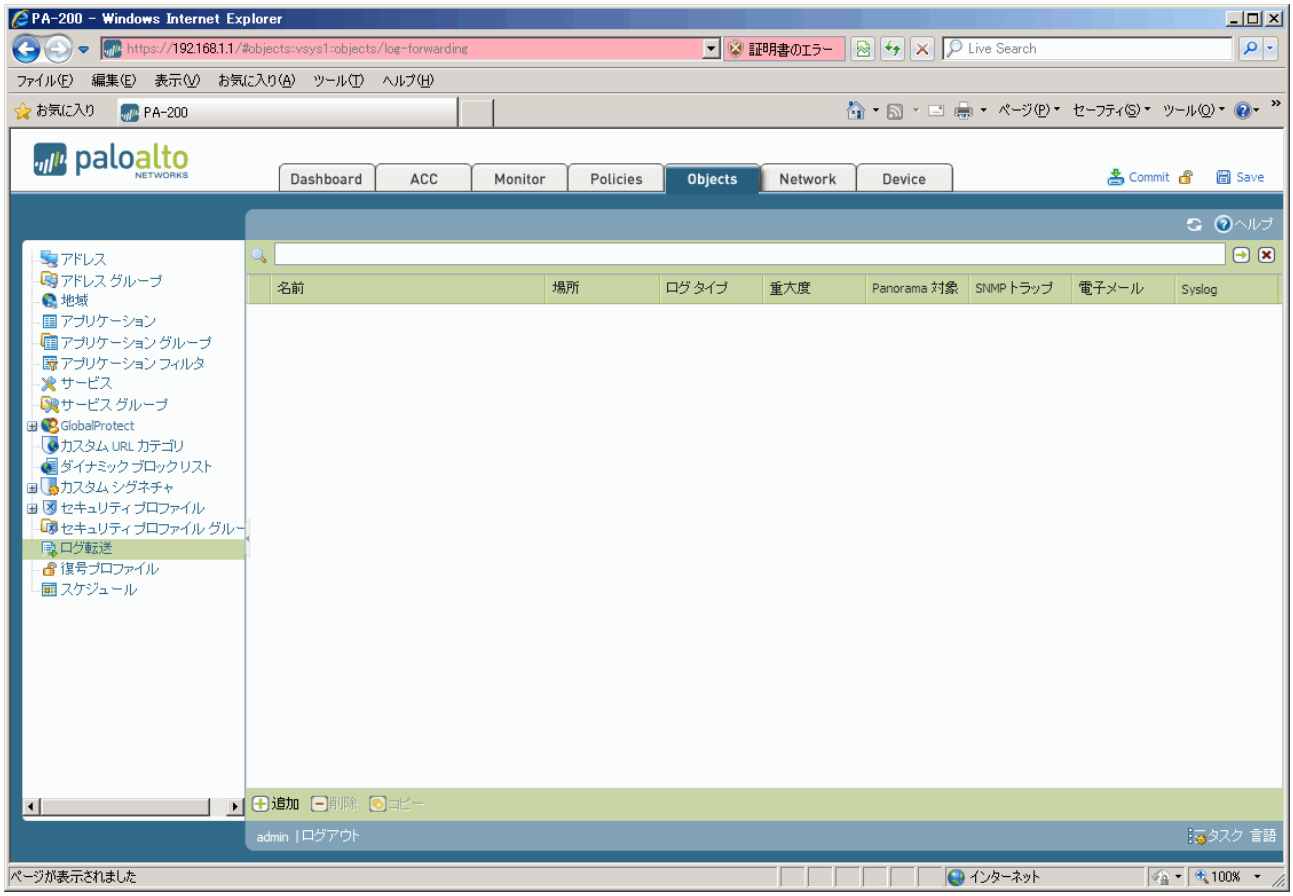


図 11 [ログ転送]ウィンドウ

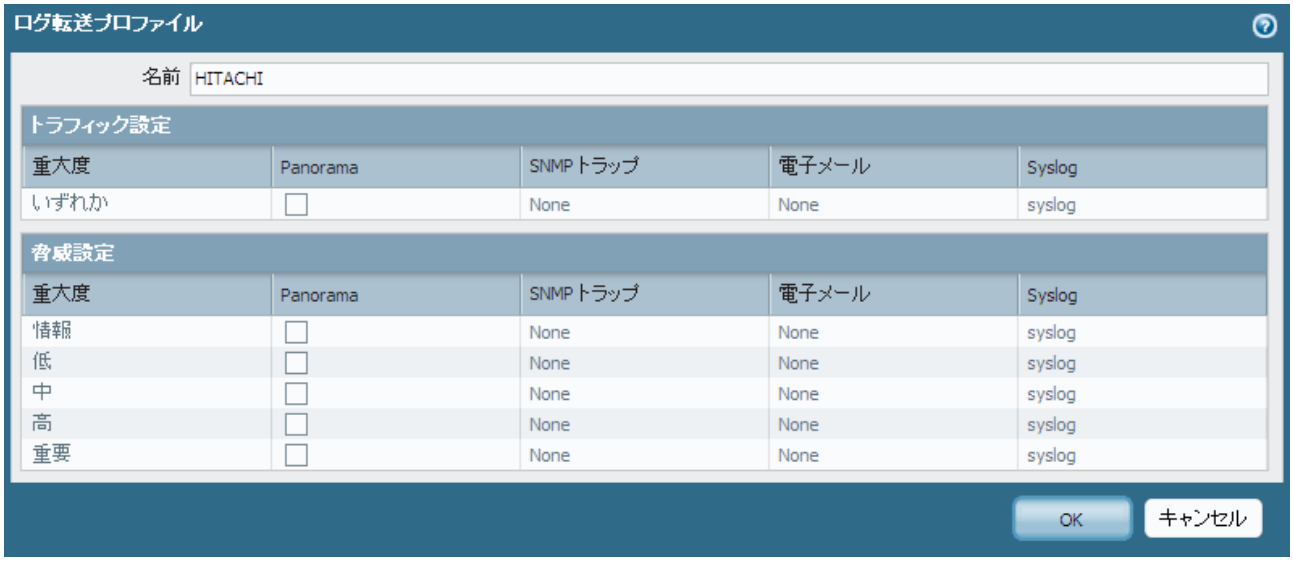


図 12 [ログ転送プロファイル]ウィンドウ

- [追加]ボタンをクリックします(クリックして開かれたウィンドウを図 12 に示します)。
- [名前]を指定します。**ここで指定した名称を「名称２」とします**。

- [トラフィック設定]の[Syslog]ドロップダウンリストから，**「名称１」**を指定します。
- 表 3.1-1 を参考に，[脅威設定]の [Syslog]ドロップダウンリストから，**「名称１」**を指定します。
- 最後に，[OK]をクリックします。

表 3.1-1 ログレベル（脅威）

ログレベル	FIREWALLstaff に関連するログ
情報	攻撃，ウイルス，URL フィルタ
低	攻撃，ウイルス
中	攻撃，ウイルス
高い	攻撃，ウイルス
重要	攻撃，ウイルス

(2) ポリシ毎のログ出力の設定

すでに設定されている Palo Alto の各ポリシに，ログを出力する設定を行います。

[Policies]-[セキュリティ]を選択します（図 13 参照）。

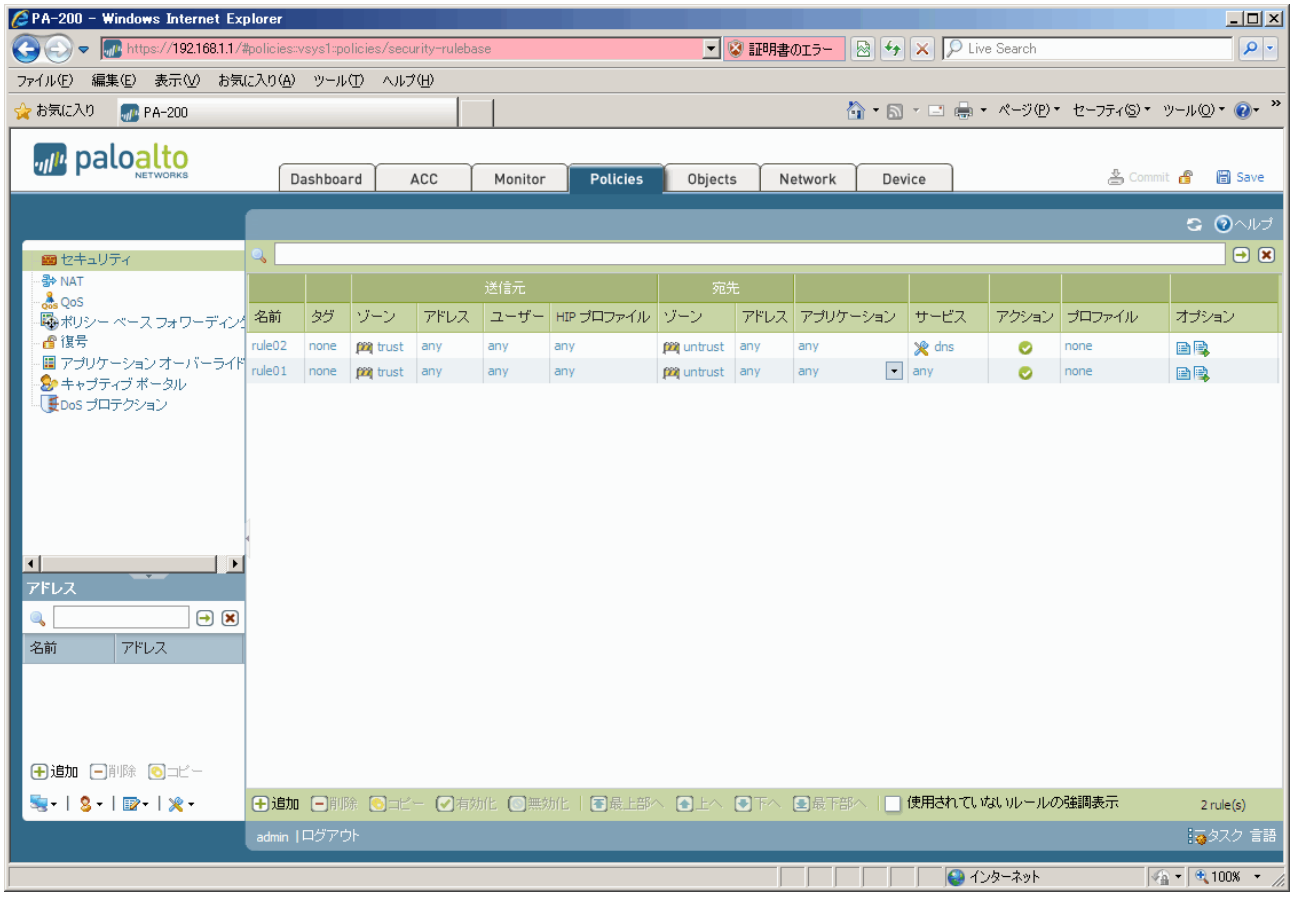


図 13 [セキュリティ]ウィンドウ

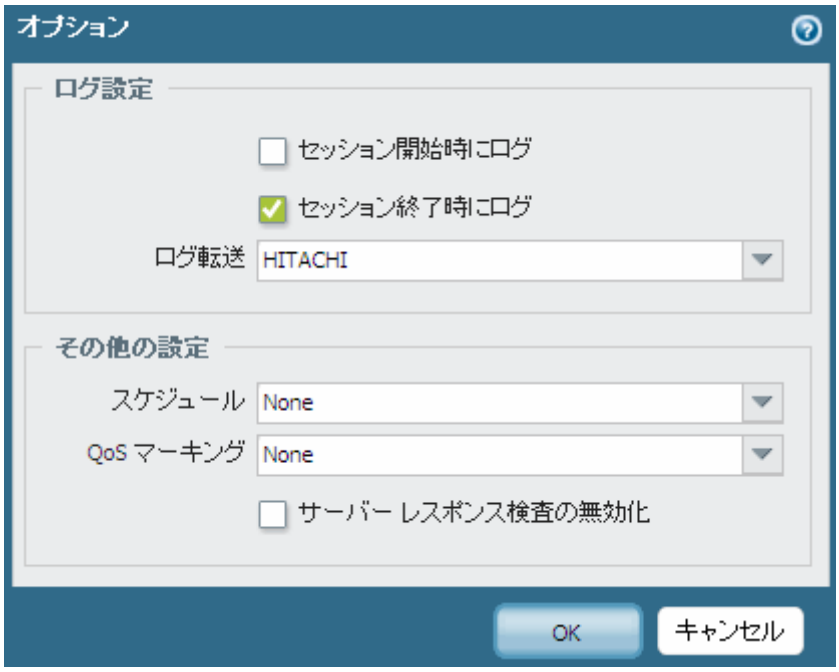


図 14 [オプション]ウィンドウ

- ログを送信するポリシの[オプション]をクリックします（クリックして開かれたウィンドウを図 14 に示します）。
- [セッション終了時にログ]を選択します。
- [ログ転送]ドロップダウンリストから，**「名称２」**を指定します。
- 最後に，[OK]をクリックします。

4 Juniper SRX シリーズ

4.1 Juniper SRX シリーズの設定

4.1.1 サポート機種，OS バージョン

Juniper SRX シリーズのファイアウォールで，JUNOS が JUNOS10.0～20.4R3 のいずれかであるファイアウォール。

4.1.2 設定手順

SRX のログを解析してレポートするために必要な，SRX の設定について説明します。GUI で設定できることについては GUI を用いた設定手順を説明しますので，CUI を用いて設定する場合は，SRX のマニュアルをご参照ください。

なお，JUNOS12.1 における設定手順を説明しておりますので，他の JUNOS の場合は，SRX のマニュアルなどもあわせてご参照ください。

(1) Syslog 送信の設定

SRX から，ログ（Syslog）を送信する設定を行います。

- SRX にログインし，コンフィグレーションモードに切り替えます
- SRX から出力されるログフォーマットに，Syslog 形式を指定します
- 表 4.1-1 を参考に，次のコマンドで Syslog を受信するマシン（例，FIREWALLstaff AE Server をインストールしたマシン）に必要なログを送信するよう設定します

```
set system syslog host IPaddress Facility Priority
```

IPaddress：FIREWALLstaff AE Server の IP アドレス
Facility：ファシリティ
Priority：プライオリティ

- ログに「年」が出力されるように設定します

```
set system syslog time-format year
```

例

```
root@%
root@% cli↵
root> configure↵
root# set security log format syslog↵
root# set system syslog host 192.168.1.33 user info↵
root# set system syslog host 192.168.1.33 daemon warning↵
root# set system syslog time-format year↵
```

表 4.1-1 ログレベル

ファシリティ	プライオリティ	FIREWALLstaff に関連するログ
user	emergency	
	alert	
	critical	
	error	攻撃（IDS）
	warning	ウイルス
	notice	
	info	トラフィック，攻撃（IDP），スパム
daemon	emergency	
	alert	
	critical	
	error	
	warning	URL フィルタ
	notice	
	info	

(2) ポリシ毎のログ出力の設定

すでに設定されている SRX の各ポリシに，ログを出力する設定を行います。

[Configure]－[Security]－[Policy]－[Apply Policy]を選択します（図 15 参照）。

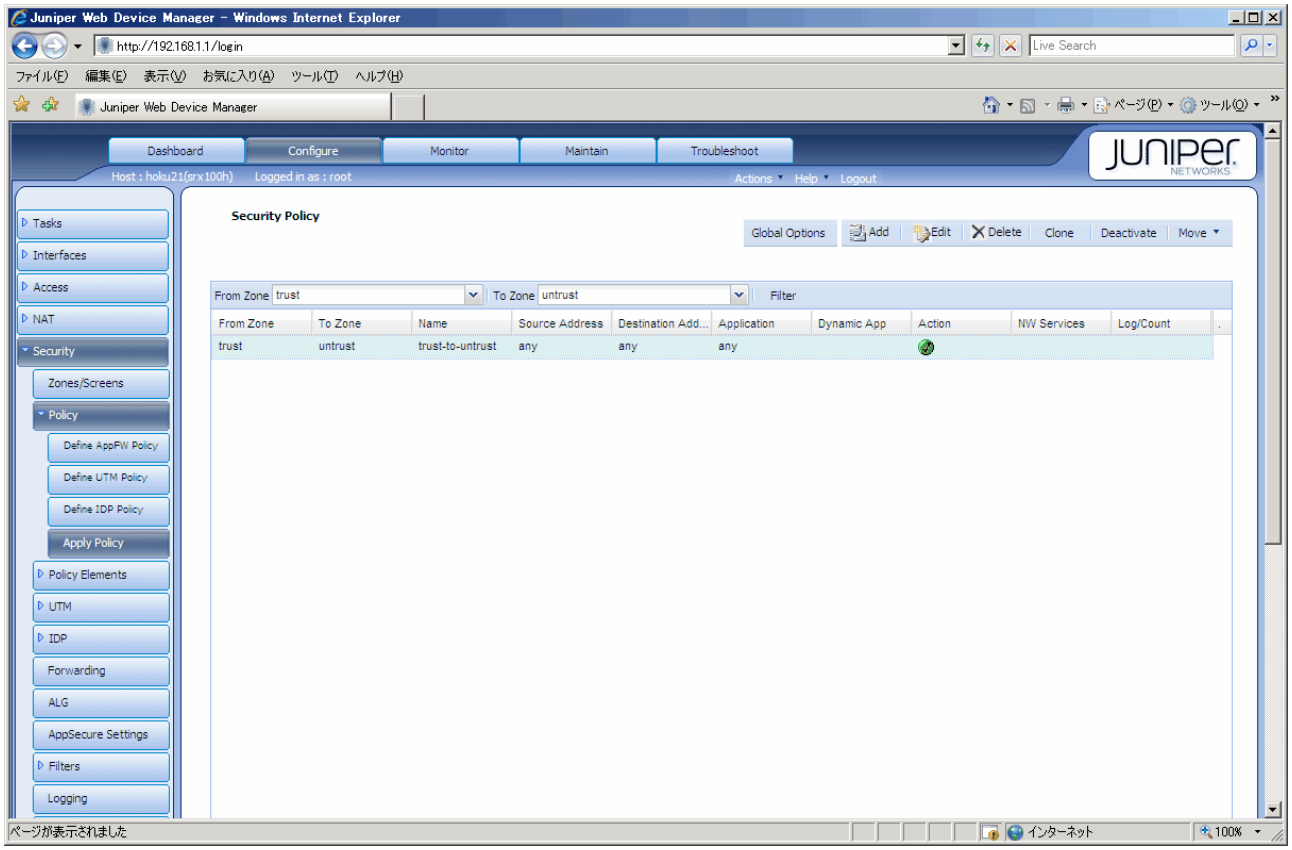


図 15 [Apply Policy]ウィンドウ

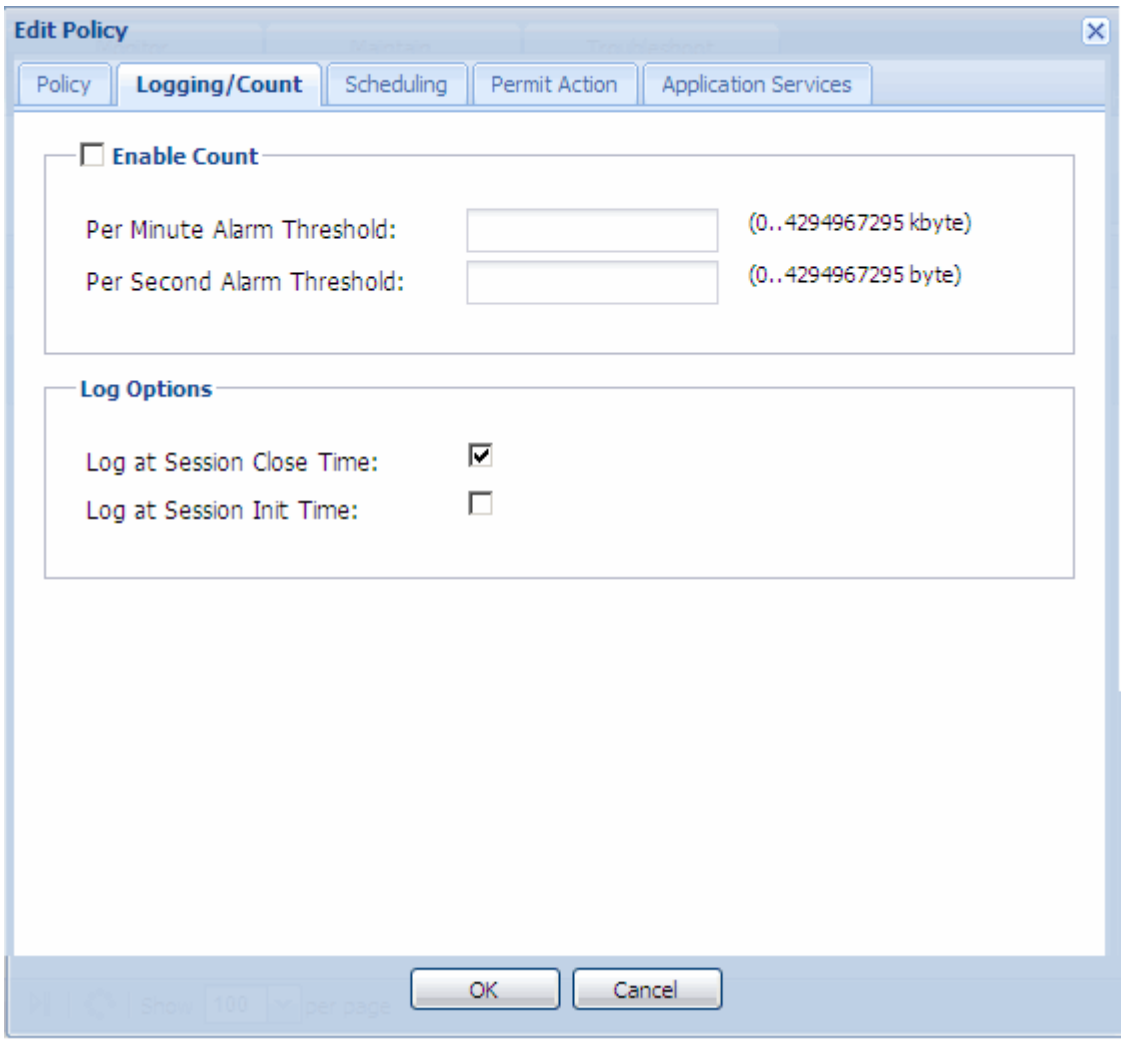


図 16 [Edit Policy]ウィンドウ

- ログを送信するポリシを選択して[Edit]をクリックします。
- [Logging/Count]タブを選択します（選択したウィンドウを図 16 に示します）。
  - ・[Policy]タブの[Policy Action]の値が permit の場合，[Log at Session Close Time]を選択します
  - ・[Policy]タブの[Policy Action]の値が deny または reject の場合，[Log at Session Init Time]を選択します
- 最後に，[OK]をクリックします。

(3) IDP のログ出力の設定

IDP のログを出力する設定を行います。

[Configure]－[Security]－[Policy]－[Define IDP Policy]を選択します（図 17 参照）。

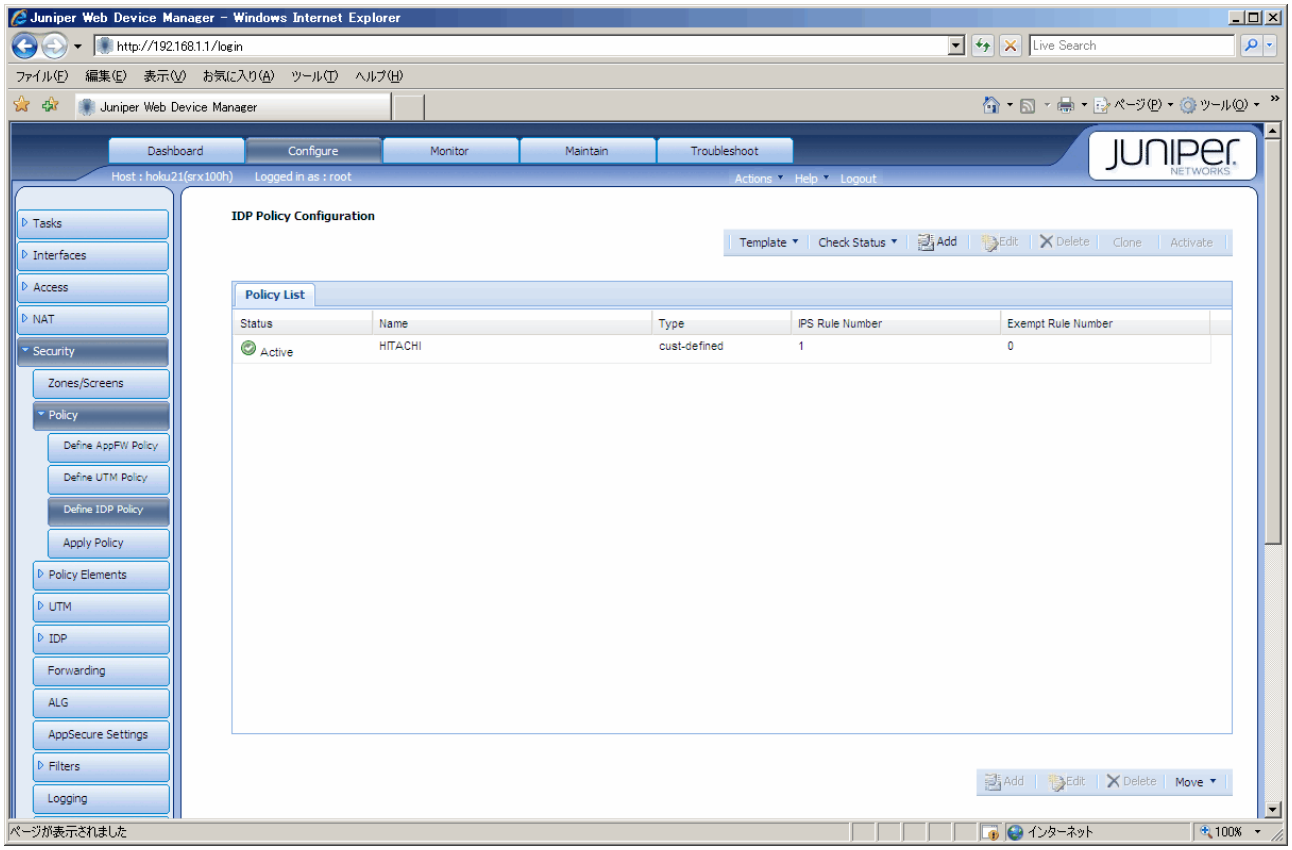


図 17 [Define IDP Policy]ウィンドウ

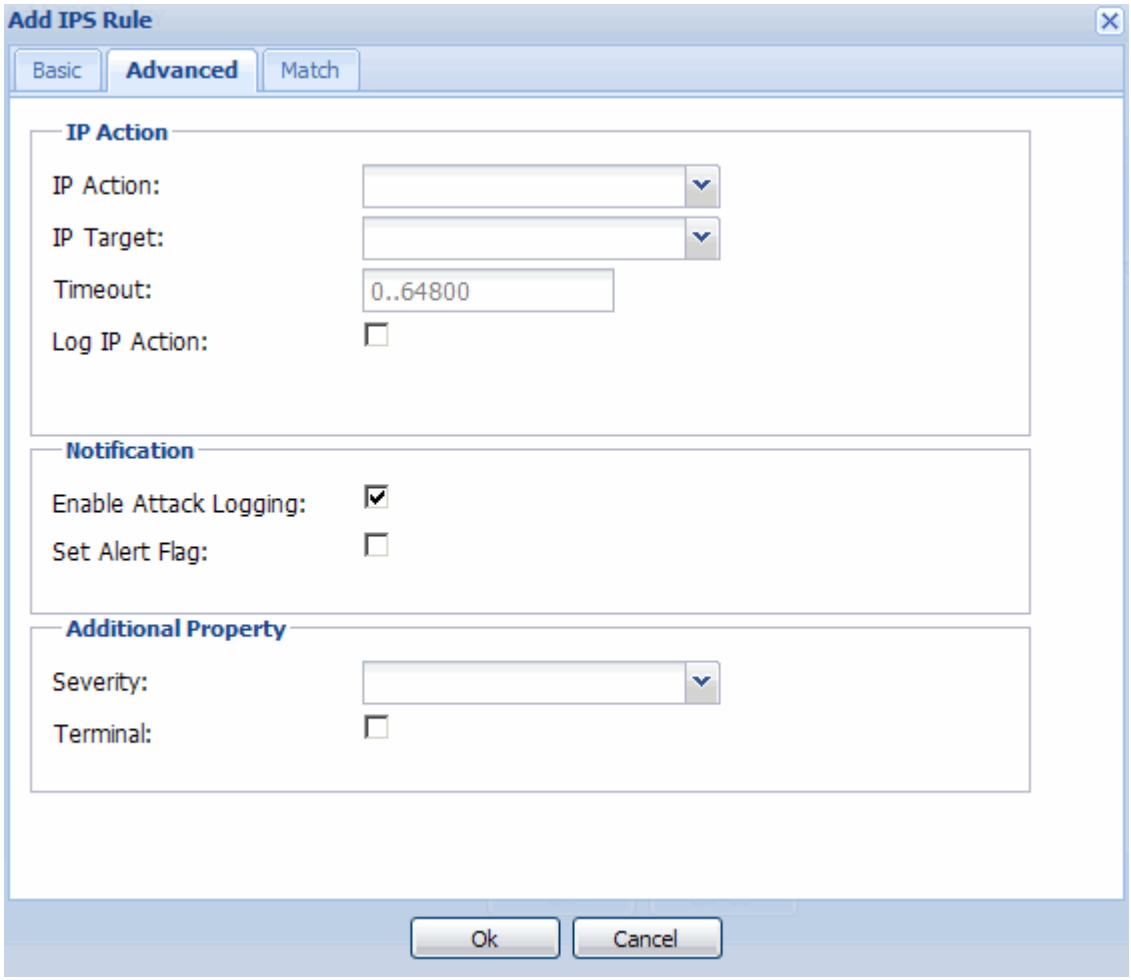


図 18 [Add IPS Rule]ウィンドウ

- [Policy List]の[Active]欄が選択されている[Name]をクリックします（クリックしたウィンドウを図 17 に示します）。
- [Rulebase:IPS]で，ログを出力する[Name]をクリックし，[Edit]をクリックします（クリックして開かれたウィンドウを図 18 に示します）。[Advanced]タブの[Enable Attack Logging]を選択して，[OK]をクリックします。この操作を，ログを出力する[Name]すべてに繰り返します。
- 最後に，[OK]をクリックします。

5 CheckPoint シリーズ

5.1　CheckPoint シリーズの設定

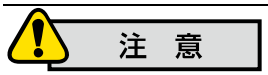
5.1.1　サポート機種，OS バージョン

CheckPoint Software Blade のファイアウォール。対応範囲は R70～R81。

5.1.2　設定手順

CheckPoint のログを LEA 接続を用いてレポートするために必要な，CheckPoint の設定について説明します。

なお，R75 における設定手順を説明しておりますので，他の場合は，CheckPoint のマニュアルなどもあわせてご参照ください。



Check Point のログを LEA 接続を用いて取得する場合，Check Point 側で 3DES を有効にする必要があります。

しかし，Check Point のバージョンにより，3DES が無効となっている場合があります。その場合，Check Point にて 3DES を有効にしてください。

3DES の有効･無効の設定方法については，Check Point の購入先にお問い合わせください。

(1) FIREWALLstaff からのアクセスの設定

CheckPoint ファイアウォールに FIREWALLstaff からアクセスできるよう，CheckPoint で設定を行います。FIREWALLstaff では，CheckPoint への接続方法として OPSEC LEA による sslca を用いた接続のみ，サポートしています。

(a) FIREWALLstaff をインストールするホストの設定

(ア) SmartDashboard を起動します。

(イ) SmartDashboard の左ペインで，[Network Objects]-[Nodes]を選択して，右クリックして[Node]-[Host...]を選択します。

(ウ) [Host Node]ダイアログの左ペインで[General Properties]を選択し，右ペインの[Name]に適切な名称を，[IP Address]に FIREWALLstaff インストール先の IP アドレスを指定します。

注 意

(ウ)で設定したホストから LEA によるログの取得が可能になるようにルールの設定が必要です。既に接続が可能となるルールが存在する場合は新たに追加する必要はありません。

設定する場合は SOURCE に(ウ)で設定したホストを，DESTINATION に FIREWALLstaff からのアクセスを許可する CheckPoint ファイアウォールを，SERVICE に LEA 接続に使用するポート番号（デフォルトで TCP の 18184）を，ACTION に accept を指定します。

(b) LEA 接続の設定

(ア) SmartDashboard を起動します。

(イ) SmartDashboard の左ペインで，[Servers and OPSEC Applications]-[OPSEC Applications]を選択して，右クリックして[New]-[OPSEC Application...]を選択します。

(ウ) [OPSEC Application Properties]ダイアログの[Name]に，適切な名称を指定します。**この値を，「OPSEC LEA アプリケーション名」と呼びます。**

(エ) ([OPSEC Application Properties]ダイアログの) [Host]に，「(a) FIREWALLstaff をインストールするホストの設定」で設定したホストを選択します。

(オ) ([OPSEC Application Properties]ダイアログの) [Client Entities]の[LEA]チェックボックスを選択します。

(カ) ([OPSEC Application Properties]ダイアログの) [Secure Internal Communication]の[Communication...]をクリックします。

(キ) [Communication]ダイアログで，[Activation Key]テキストボックスと[Confirm

Activation Key]テキストボックスに，接続のための認証キー（文字列）を入力し，[Initialize]をクリックします。

(ク)（[Communication]ダイアログの）[Trust state]が「Initialized but trust not established」であることを確認して[Close]をクリックします。

(ケ)（[OPSEC Application Properties]ダイアログの）[OK]をクリックして閉じます。そして，再度，[OPSEC Application Properties]ダイアログを開きます。[Secure Internal Communication]の[DN]の値をメモします。**この値を，「LEA SIC 名」と呼びます。**

値の例）CN=hitachi,O=cpmodule..uvwxyz

(コ)(ケ)の値（LEA SIC 名）の「,」で区切られた値の前部分を「cn=cp_mgmt」で置き換えた値をメモします。**このメモした値を，「管理サーバ SIC 名」と呼びます。**

値の例）cn=cp_mgmt,O=cpmodule..uvwxyz

(サ)（[OPSEC Application Properties]ダイアログの）[OK]をクリックします。

(シ)SmartDashboard の[Policy]-[Install]で，ポリシをインストールします。

「LEA SIC 名」「管理サーバ SIC 名」の値は，FIREWALLstaff の「ファイアウォールの設定パネル」の[ファイアウォール *n*]フィールドに設定します。

(2) ログ出力の設定

SmartDashboard を起動し,必要なログを出力するように設定します。

(a) アクセス制御ポリシ

[Firewall]タブをクリックし，ログ出力するアクセス制御ポリシの TRACK を，次のように設定します。

ACTION の値	TRACK で指定する値
accept	Account
drop	Log
reject	Log

(b) その他

必要に応じて，UTM 関連のログを出力するように設定します。

- IPS
- Anti-Virus
- Anti-Spam
- URL Filtering
- Application

5.2 opsec.p12 ファイルの作成

FIREWALLstaff をインストールしたコンピュータで，opsec.p12 ファイルを作成し，配置する必要があります。

以下の手順で，opsec.p12 ファイルを作成してください。以降の説明で使用するパス置換文字を表 5.2-1 に示します。

表 5.2-1 パス置換文字

#	パス置換文字	説明
1	%DATA_DIR%	FIREWALLstaff インストール時に指定したデータフォルダの絶対パスを示します。
2	%INSTALL_DIR%	FIREWALLstaff インストール時に指定したインストールフォルダの絶対パスを示します。
3	%FW_ID%	ファイアウォール識別子を示します。
4	%FWx%	ファイアウォール 1 の設定を行う場合は「FW1」が，ファイアウォール 2 の設定を行う場合は「FW2」が対応します。

(ア) コマンドプロンプトを開きます。

(イ) 「opsec_pull_cert.exe」コマンドを用いて「opsec.p12」ファイルを作成します。コマンドの書式と引数の説明は以下の通りです。

opsec_pull_cert.exe -h CheckPoint_IP -n LEA_object -p text_string

変数名	内容
CheckPoint_IP	CheckPoint ファイアウォールの IP アドレス
LEA_object	「5.1.2(1)(b) LEA 接続の設定 (ウ)」で指定した，OPSEC LEA アプリケーション名
text_string	「5.1.2(1)(b) LEA 接続の設定 (キ)」で指定した，認証キー

「opsec_pull_cert.exe」は%INSTALL_DIR%¥lea フォルダに存在するので実行する際は絶対パスで指定してください。

例)

”C:¥Program Files¥HitachiSolutions¥FIREWALLstaff¥lea¥opsec_pull_cert.exe” -h 192.168.1.1 -n hitachi -p pass0001

(ウ) 成功した場合は以下のような応答が表示され実行フォルダに「opsec.p12」というファイルが作成されます。

```
The full entity sic name is:
CN=hitachi,O=cpmodule..uvwxyz
Certificate was created successfully and written to "opsec.p12".
```

(エ) 「opsec.p12」ファイルを，以下のフォルダに配置します。

%DATA_DIR%¥firewall¥lea¥%FW_ID%¥%FWx%

例）C:¥HitachiSolutions¥FIREWALLstaff¥Data¥firewall¥lea¥FW001¥FW1

チェックポイントから発行を受けた証明書（opsec.p12）には有効期間（およそ 5 年）がありますので，定期的に再作成してください。再作成の手順は以下の通りです

1. FIREWALLstaff Log サービスを停止し，既存の証明書（opsec.p12）を別フォルダにバックアップします。
2. チェックポイントの SmartDashboard で，FIREWALLstaff が接続している LEA オブジェクトに対して，[Edit] - [Communication] - [Reset]を実施し認証キー（Authentication Key）を入力し直した後，ポリシーを再インストールします。
3. 「(ア)」～「(エ)」を実行して証明書（opsec.p12）を作成します。
4. FIREWALLstaff Log サービスを開始します。

5.3 エクスポートログについて

FIREWALLstaff では，CheckPoint の「fwm logexport」コマンドを用いてエクスポートしたログファイルを用いてレポートを作成することができます。

例）「myout.log」というファイル名でエクスポートする場合

```
fwm logexport -n -o myout.log
```

・ 「-n」オプションは，名前解決を行わないようするオプションです。
FIREWALLstaff AE Server のプロファイル画面内の[ファイアウォールの設定]パネルにて，内部ネットワークまたは DMZ ネットワークの設定を IP アドレスで指定する場合は，名前解決を行わないオプションを指定してください。

コマンドの使用方法の詳細は，CheckPoint のマニュアルを参照ください。

6 IPCOM EX IN/SC シリーズ

6.1 IPCOM EX IN/SC シリーズの設定

6.1.1 サポート機種，OS バージョン

IPCOM EX IN/SC シリーズのファイアウォールで，OS が E10L50～E20L31 のいずれかであるファイアウォール。

6.1.2 設定手順

IPCOM のログを解析してレポートするために必要な，IPCOM の設定について説明します。

(1) Syslog の設定

IPCOM から，ログ（Syslog）を送信する設定を行います。

[設定]－[運用管理設定]－[ログ]－[ログ転送]の「ログ転送ルール一覧」で，以下を指定します。

- 「ログ転送設定」で，「フォーマット形式」に「IPCOM 形式」を指定
- 「Syslog 転送設定一覧」で，「転送先」に Syslog を受信するマシン（例，FIREWALLstaff をインストールしたマシン）の IP アドレスを指定

[設定]－[運用管理設定]－[ログ]－[ログ採取]の「タイムスタンプ情報」で，「追加する」を指定します。

(2) ログ出力の設定

FIREWALLstaff は，表 6.1-1 で示すメッセージを解析対象としています。解析する目的に応じて，メッセージを出力するよう設定してください。各メッセージの出力方法は，IPCOM の「コンソールリファレンスガイド」などをご参照ください。

表 6.1-1 メッセージ一覧

分類	メッセージ ID	ログ種別	重大度	備考
通常通信	00300005	セッションログ	INFO	「アクセス制御ルール」によってアクセス制御を行っている場合 **注意１ 参照**
	00300007	セッションログ	INFO	
	00300009	セッションログ	INFO	
	00309005	セッションログ	INFO	「アクセス制御マップ」によってアクセス制御を行っている場合 **注意２ 参照**
	00309007	セッションログ	INFO	
	00309003	セッションログ	INFO	
拒否通信	40300011	セッションログ	WARNING	「アクセス制御ルール」によってアクセス制御を行っている場合 **注意１ 参照**
	40300013	セッションログ	WARNING	
	40300015	セッションログ	WARNING	
	40309011	セッションログ	WARNING	「アクセス制御マップ」によってアクセス制御を行っている場合 **注意２ 参照**
	40309013	セッションログ	WARNING	
	40309015	セッションログ	WARNING	
アノマリ型 IPS **注意３ 参照**	C0304001	セッションログ	CRITICAL	TCP ポートスキャン
	C0304003	セッションログ	CRITICAL	UDP ポートスキャン
	C0304005	セッションログ	CRITICAL	ホストスキャン
	C0305001	セッションログ	ALERT	SYN Flood 攻撃
	C0305003	セッションログ	ALERT	ICMP Flood 攻撃
	C0305005	セッションログ	ALERT	UDP Flood 攻撃
	C0305007	セッションログ	ALERT	UDP Bomb 攻撃
	C0305009	セッションログ	ALERT	Very Small IP Fragment 攻撃
	C0305011	セッションログ	ALERT	Too Many IP Fragment 攻撃
	C0305013	セッションログ	ALERT	Fragmented ICMP 攻撃
	C0305015	セッションログ	ALERT	Fragmented IGMP 攻撃
	C0305017	セッションログ	ALERT	Empty Fragment 攻撃
	C0305019	セッションログ	ALERT	Over lapped Fragment 攻撃
	C0305021	セッションログ	ALERT	Large ICMP 攻撃
	C0305023	セッションログ	ALERT	Ping of Death 攻撃
	C0305025	セッションログ	ALERT	IP Spoofing 攻撃
	C0305027	セッションログ	ALERT	Land 攻撃
	C0305029	セッションログ	ALERT	Smurf 攻撃
	C0305031	セッションログ	ALERT	Unrequested ICMP Echo Reply 攻撃

	C0305033	セッションログ	ALERT	Fraggle 攻撃
	C0305035	セッションログ	ALERT	FTP Bounce 攻撃
	C0305037	セッションログ	ALERT	Snork 攻撃
	C0305039	セッションログ	ALERT	Winnuke 攻撃
	C0305041	セッションログ	ALERT	URL Overflow 攻撃
	C0305043	セッションログ	ALERT	Spam Mail 攻撃
	C0305045	セッションログ	ALERT	MIME Overflow 攻撃
	C0305047	セッションログ	ALERT	Very Small TCP Segment 攻撃
シグネチャ型 IPS	803E9004	セッションログ	ERROR	検知
	403E9104	セッションログ	WARNING	検知
	003E9204	セッションログ	NOTICE	検知
	003E9304	セッションログ	INFO	検知
	803E9000	セッションログ	ERROR	防御
	403E9100	セッションログ	WARNING	防御
	003E9200	セッションログ	NOTICE	防御
	003E9300	セッションログ	INFO	防御
WAF 脆弱性攻撃	40587001	WAF ログ	WARNING	ディレクトリトラバーサル攻撃
	40587002	WAF ログ	WARNING	XSS 攻撃
	40587003	WAF ログ	WARNING	SQL インジェクション攻撃
	40587004	WAF ログ	WARNING	OS コマンドインジェクション攻撃
	40587005	WAF ログ	WARNING	SSI インジェクション攻撃
ウイルス	403A0001	ウイルスログ	WARNING	SMTP
	403A0002	ウイルスログ	WARNING	HTTP
	403A0003	ウイルスログ	WARNING	POP3
	403A0004	ウイルスログ	WARNING	FTP
アンチスパム	403A0001	ウイルスログ	WARNING	SMTP
	403A0003	ウイルスログ	WARNING	POP3
URL フィルタリング	003B0001	セッションログ	INFO	

注 意 1

[設定]－[装置設定]－[ファイアウォール（アクセス制御）]の「アクセス制御ルール一覧」で，各インタフェースの

方向：入力

の各ルールに対して出力されたログを解析対象とします。

注 意 2

［設定］－［装置設定］－［ファイアウォール（アクセス制御）］の「インターフェースグループ／アクセス制御マップ一覧」で，「対象コネクション」が

入力方向(inbound)

IPsec トンネル内からの入力方向(in-decrypted)

の「アクセス制御マップ」に指定された各ルールに対して出力されたログを解析対象とします。

注 意 3

［設定］－［装置設定］－［IPS］－［アノマリ型 IPS］の「アノマリ型 IPS ルール一覧」で，各インタフェースの

フィルタ条件：入力

の各監査種別に対して出力されたログを解析対象とします。

7 Cisco ASA シリーズ

7.1 Cisco ASA シリーズの設定

7.1.1 サポート機種，OS バージョン

Cisco ASA シリーズのファイアウォールで，OS のバージョンが 7.2～9.1 のいずれかであるファイアウォール。

7.1.2 設定手順

Cisco ASA のログを解析してレポートするために必要な，Cisco ASA の設定について説明します。ASDM を用いた設定手順を説明しますので，CUI を用いて設定する場合は，Cisco ASA のマニュアルをご参照ください。

なお，ASA Version 9.1 における設定手順を説明しておりますので，他のバージョンの場合は，Cisco ASA のマニュアルなどもあわせてご参照ください。

(1) Syslog の設定

Cisco ASA から，ログ（Syslog）を送信する設定を行います。

[Configuration]－[Device Management]－[Logging]－[Syslog Servers]を選択します（図 19 参照）。

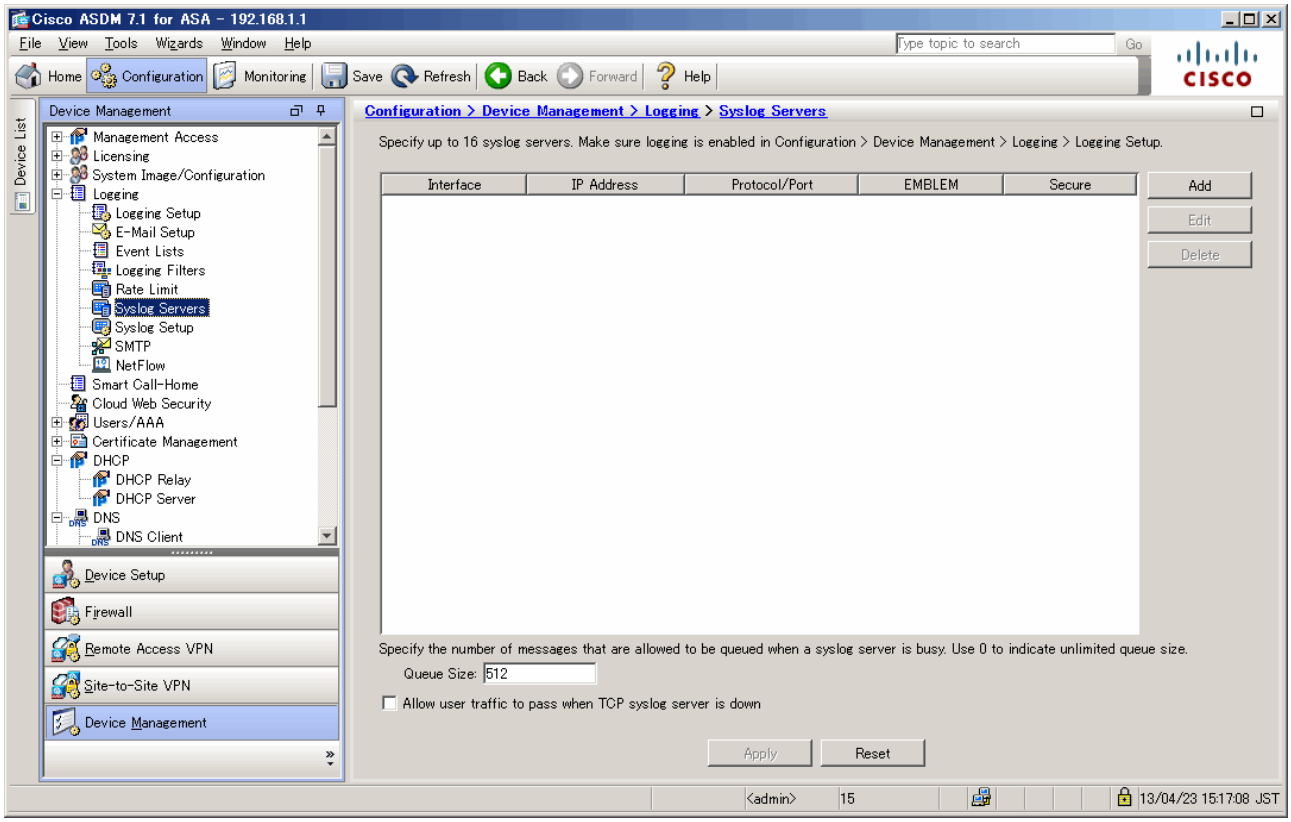


図 19 [Syslog Servers]ウィンドウ

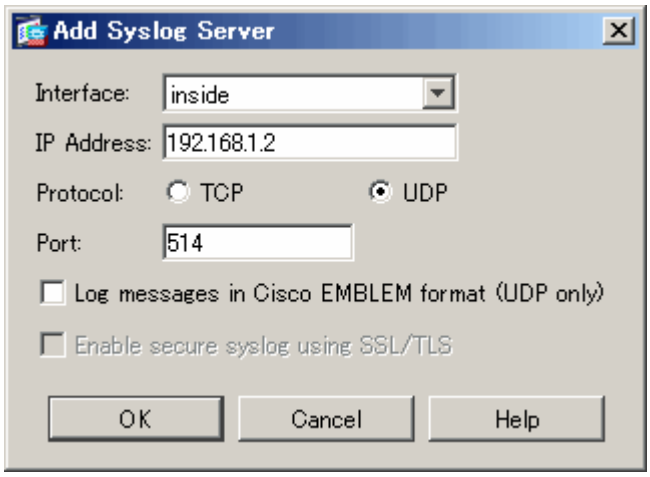


図 20 [Add Syslog Server]ダイアログ

- [Add]をクリックします（開かれたダイアログを図 20 に示します）。
- [Interface]に，Syslog を受信するマシン（例，FIREWALLstaff AE Server をインストールしたマシン）が存在しているインタフェースを指定します。
- [IP Address]に，Syslog を受信するマシンの IP アドレスを指定します。
- [Protocol]に，TCP でログを送信するか UDP でログを送信するかを指定します。
- [Port]に，Syslog を受信するマシンでの Syslog 待ちうけポート番号（通常は 514）を指定します。
- [Log messages in Cisco EMBLEM format (UDP only)]チェックボックスを**選択しません**。選択した場合，FIREWALLstaff でログの解析ができません。
- [OK]をクリックして，図 20 のダイアログを閉じます。
- 最後に，図 19 の[Apply]をクリックします。

[Configuration]－[Device Management]－[Logging]－[Syslog Setup]を選択します（図 21 参照）。

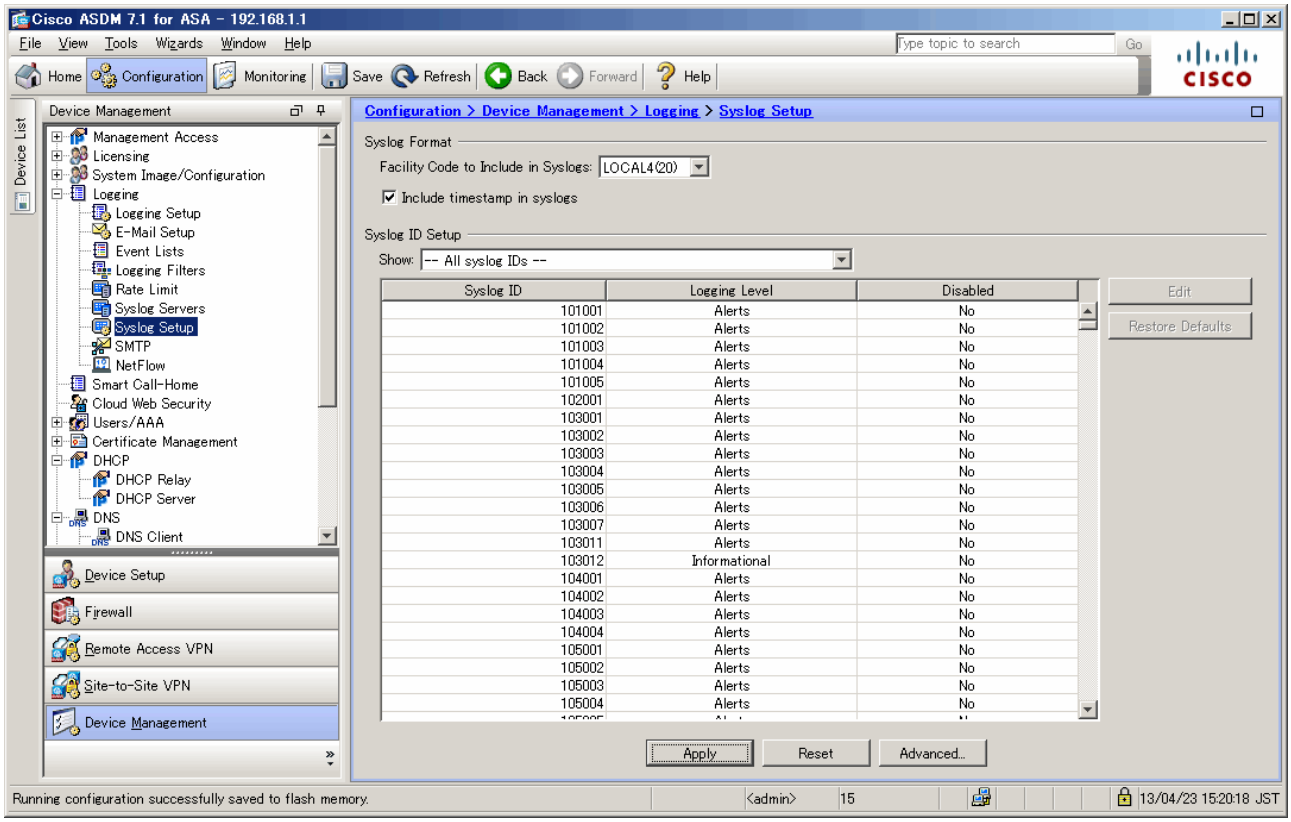


図 21 [Syslog Setup]ウィンドウ

- [Include timestamp in syslogs]チェックボックスを<u>選択します</u>。選択しないと，FIREWALLstaff でログの解析ができません。
- FIREWALLstaff は，表 7.1-1 で示すメッセージを解析対象としています。解析する目的に応じて，メッセージを出力するように各 Syslog ID の Disabled 項目を指定します。
- 最後に，[Apply]をクリックします。

表 7.1-1 解析対象メッセージ

分類	Syslog ID
通過通信	302013 と 302014
	302015 と 302016
遮断通信	106023
	106103
	109025
攻撃検知	400007～400009，400023～400028，400031～400033，400041，400050

[Configuration]－[Device Management]－[Logging]－[Logging Setup]を選択します（図 22 参照）。

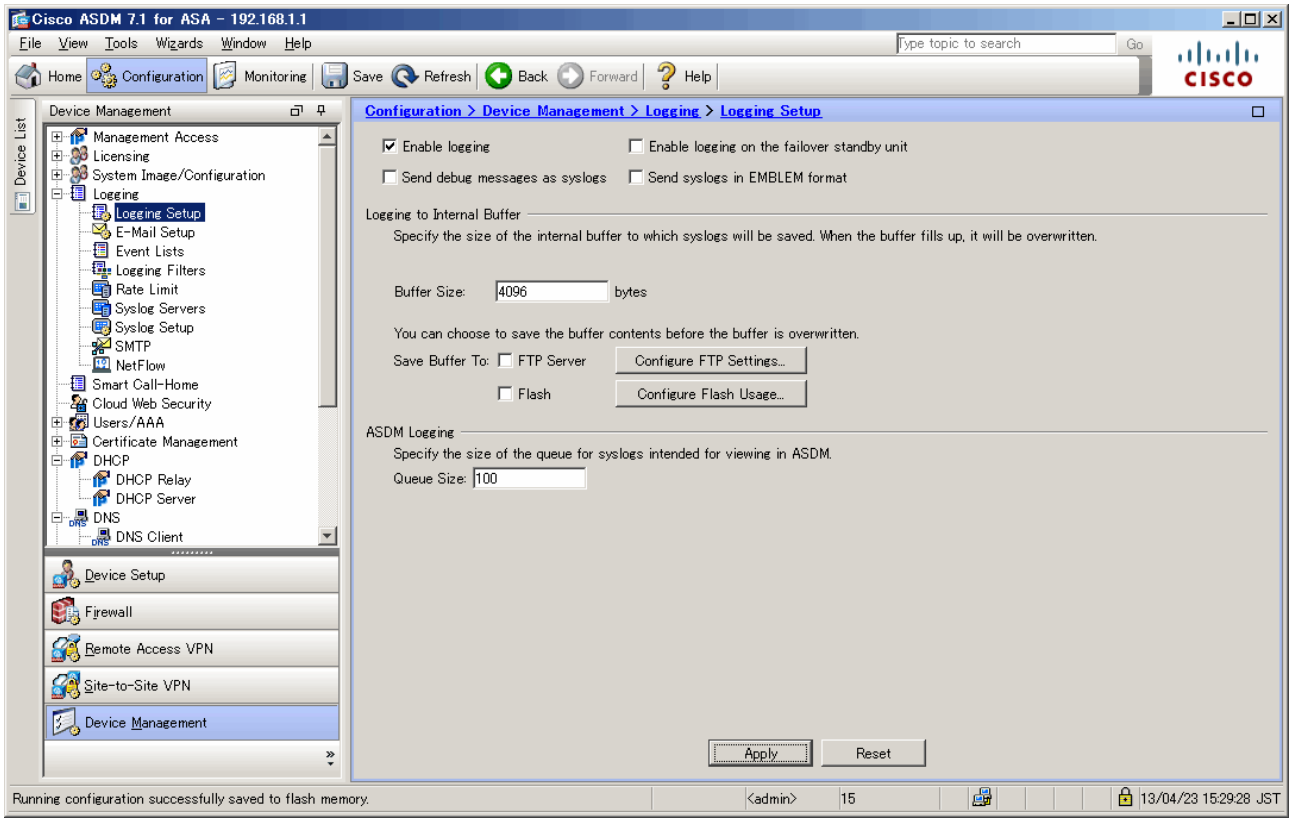


図 22 [Logging Setup]ウィンドウ

- [Enable logging]チェックボックスを選択します。
- 最後に，[Apply]をクリックします。

[Configuration]－[Device Management]－[Logging]－[Logging Filters]を選択します（図 23 参照）。

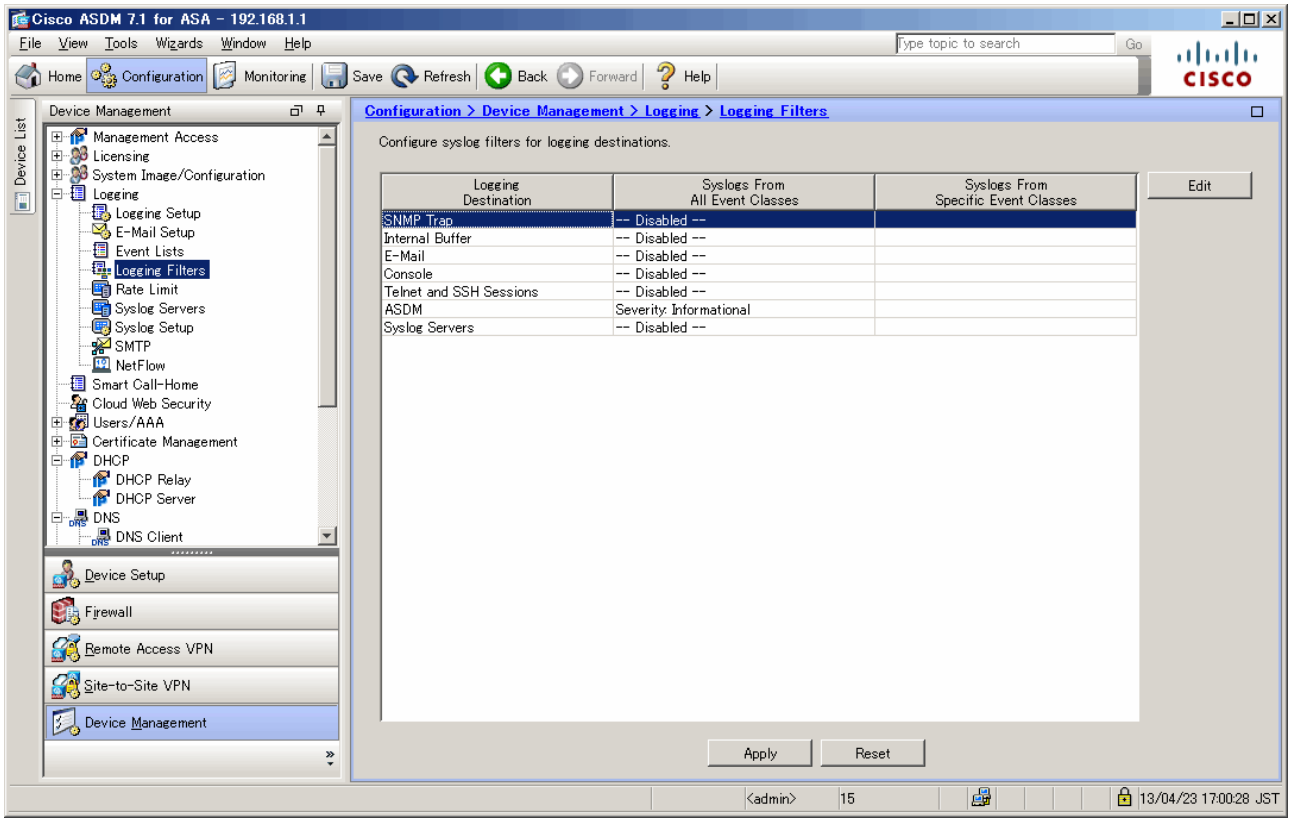


図 23 [Logging Filters]ウィンドウ

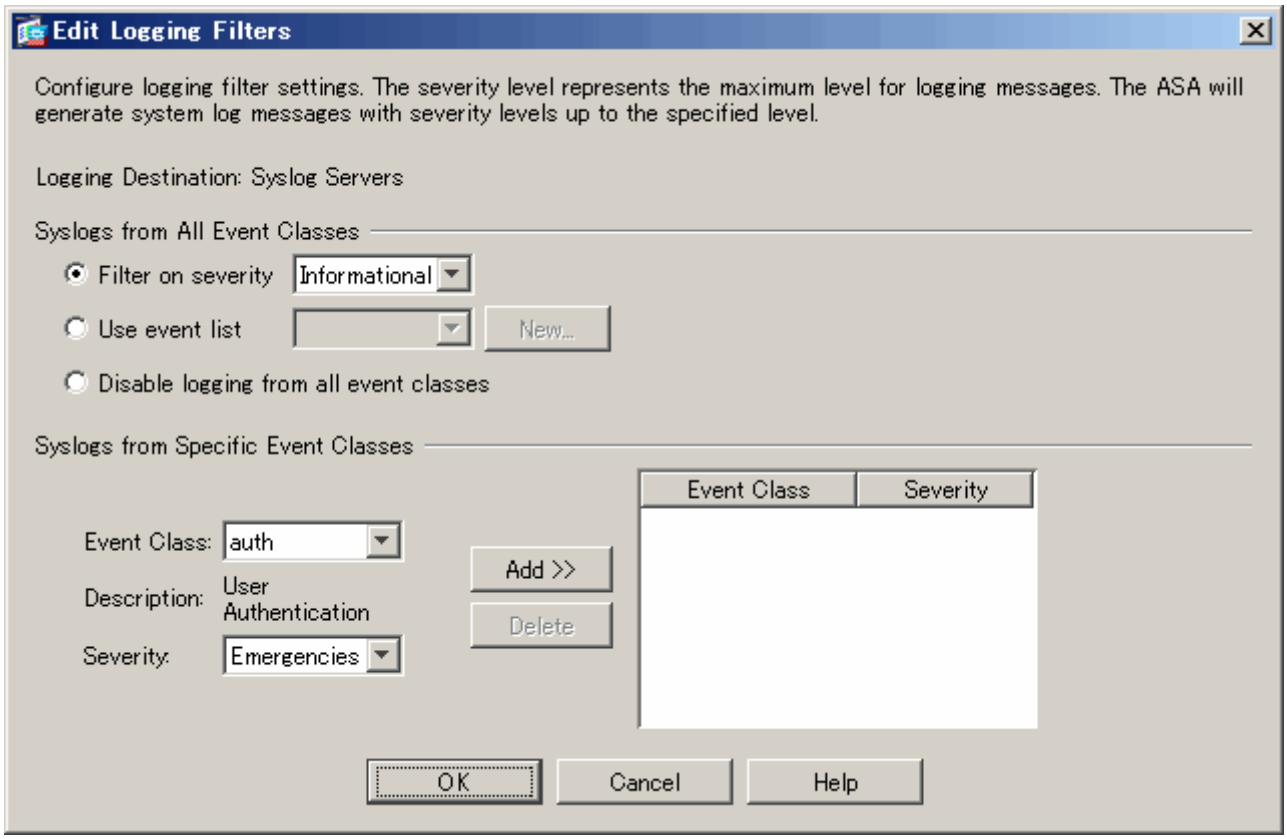


図 24 [Edit Logging Filters]ダイアログ

- Logging Destination 項目で，[Syslog Servers]を選択して[Edit]をクリックします（開かれたダイアログを図 24 に示します）。
- [Filter on severity]ラジオボタンを選択し，[Informational]を選択します。
- [OK]をクリックして，図 24 のダイアログを閉じます。
- 最後に，図 23 の[Apply]をクリックします。

(2) ポリシ毎のログ出力の設定

すでに設定されている Cisco ASA の各ポリシに，ログを出力する設定を行います。

[Configuration]－[Firewall]－[Access Rules]を選択します（図 25 参照）。

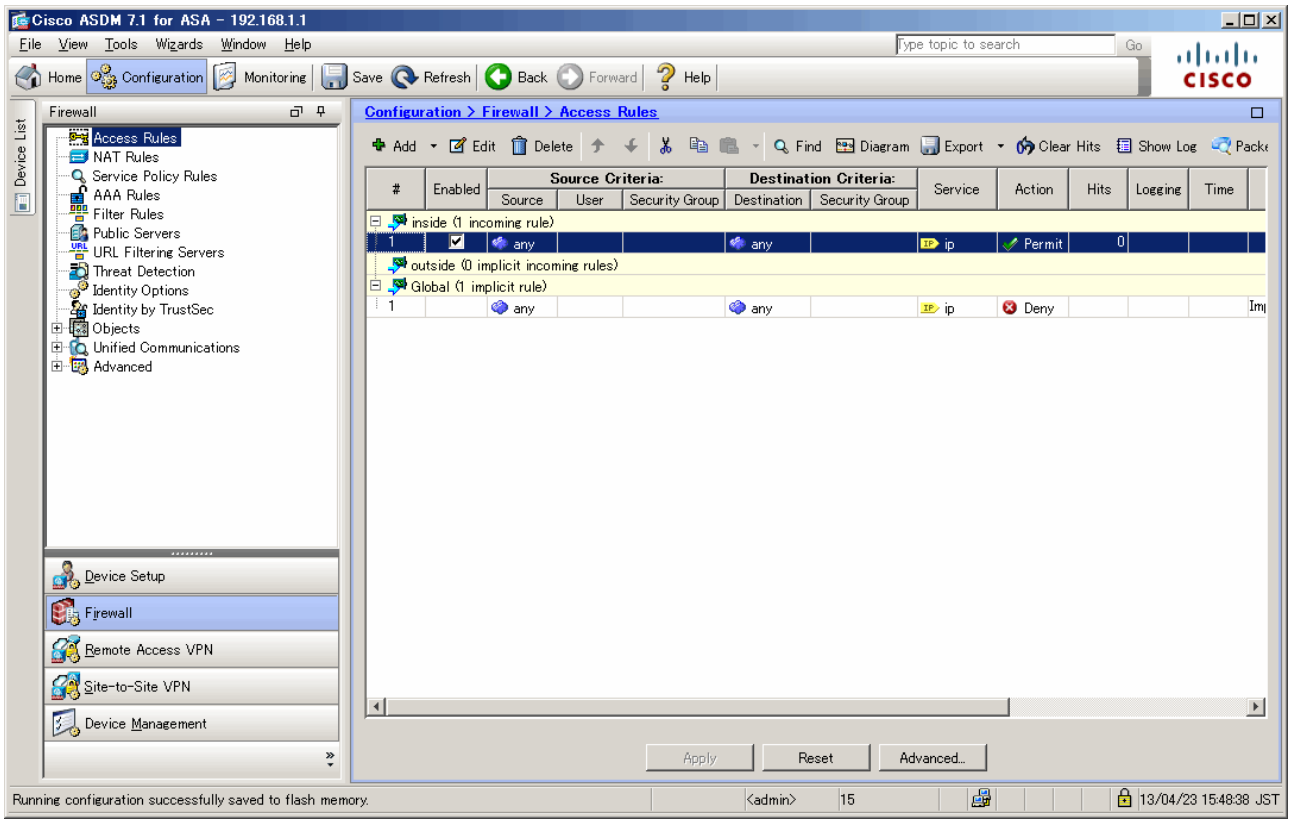


図 25 [Access Rules]ウィンドウ

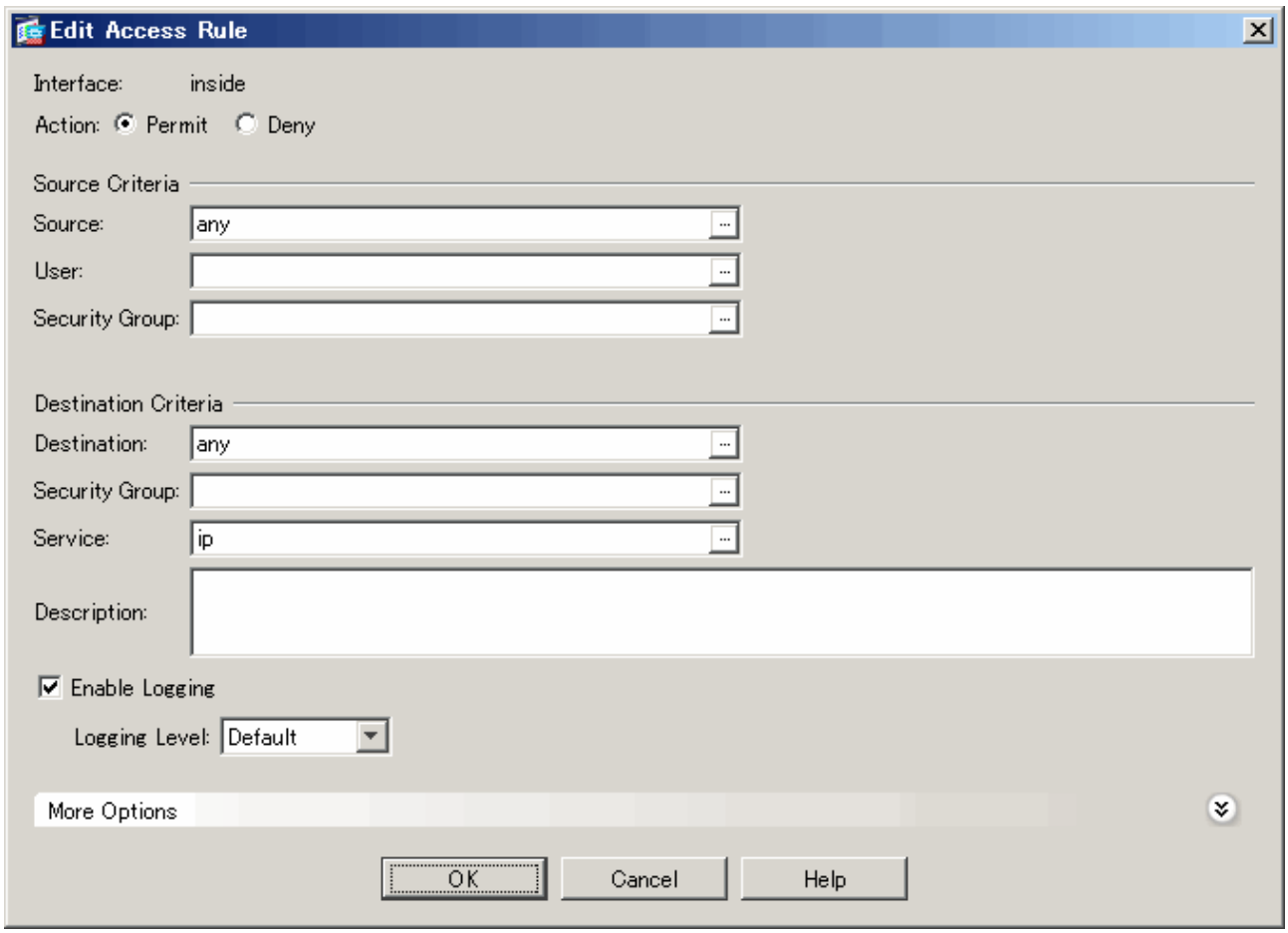


図 26 [Edit Access Rule]ダイアログ

- ログを送信するルールを選択して，[Edit]をクリックします（開かれたダイアログを図 26 に示します）。
- [Enable Logging]チェックボックスを選択します。
- [OK]をクリックして，図 26 のダイアログを閉じます。
- 最後に，図 25 の[Apply]をクリックします。

日立ソリューションズ
http://www.hitachi-solutions.co.jp/