APPENDIX D

例

この付録では、Security Management アプライアンスを実装するいくつかの一般的な方法について、図を使用して説明します。次の項目を取り上げます。

Web セキュリティ アプライアンスの例

ここでは、Security Management アプライアンスと Web セキュリティ アプライアンスの使用方法について説明します。

（注） 以下のすべてのシナリオでは、Security Management アプライアンス *および*ご使用の Web セキュリティ アプライアンスとで Web レポーティングと Web トラッキングをイネーブルにしていることを前提としています。Web レポーティ

ングと Web トラッキングをイネーブルにする方法については、Security Management アプライアンスでの中央集中型 Web レポーティングのイネーブル化とディセーブル化を参照してください。

例 1：ユーザの調査

この例では、システム管理者が会社内の特定のユーザを調査する方法について説明します。

このシナリオでは、ある従業員が勤務中に不適切な Web サイトにアクセスしている、という苦情を管理者が受け取っています。それを調査するには、システム管理者が Web アクティビティの詳細をトラッキングする必要があります。

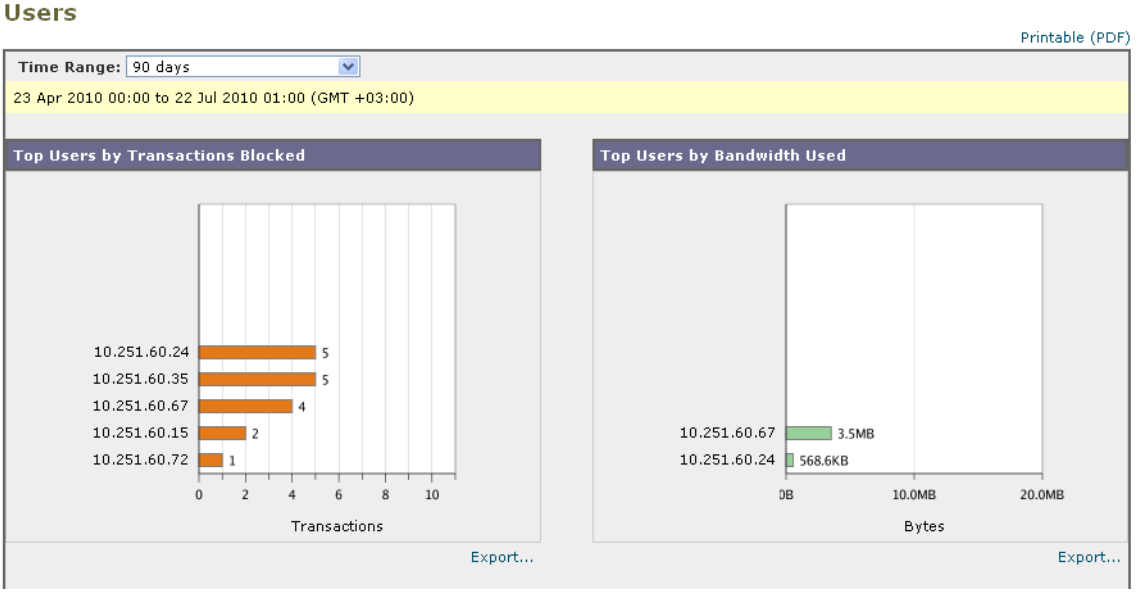
Web アクティビティがトラッキングされると、従業員の参照履歴に関する情報が記載された Web レポートが作成されます。

ステップ 1　Security Management アプライアンスで、[Web] > [Reporting] > [Users] を選択します。

[Users] ページが表示されます。

ステップ 2　[Users] テーブルで、調査する [User ID] または [Client IP address] をクリックします。

ユーザ ID またはクライアント IP アドレスがわからない場合は、ユーザ ID またはクライアント IP アドレスをわかる範囲でテキスト フィールドに入力し、[Find User ID or Client IP address] をクリックします。IP アドレスが正確に一致していなくても結果は返されます。[Users] テーブルには、入力されたユーザ ID とクライアント IP アドレスが読み込まれます。この例では、クライアント IP アドレス 10.251.60.24 の情報について検索しています。



ステップ 3　IP アドレス [10.251.60.24] をクリックします。

10.251.60.24 のユーザの詳細ページが表示されます。

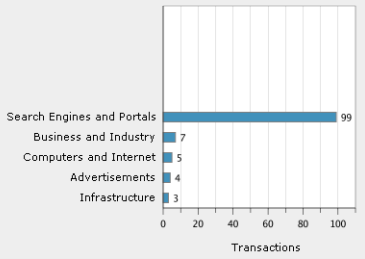
Users > 10.251.60.24

Printable (PDF)

Time Range: 90 days

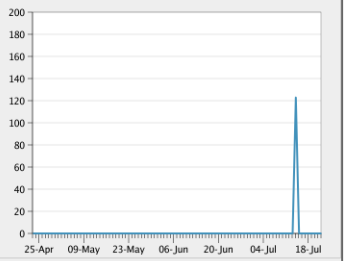
23 Apr 2010 00:00 to 22 Jul 2010 01:42 (GMT +03:00)

URL Categories by Total Transactions



Export...

Trend by Total Transactions



Export...

URL Categories Matched

URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions
Search Engines and Portals	447.4KB	00:21	0	99	99
Business and Industry	15.5KB	00:06	0	7	7
Computers and Internet	84.4KB	00:06	0	5	5
Advertisements	16.9KB	00:00	0	4	4
Infrastructure	4,540B	00:00	0	3	3
Totals (all available data):	568.6KB	00:33	0	118	118

Find URL Category

Columns... | Export...

Domains Matched

*Data below is not available for the full time range selected. Data for this table is available for **13 Jul 2010 01:00 to 14 Jul 2010 23:59 (GMT +03:00)**. Click to change the time range of this report to reflect the data available.*

Change Time Range

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
google.com	464.5KB	00:36	101	5	106
gmodules.com	83.1KB	00:06	4	0	4
google-analytics.com	8,272B	00:00	4	0	4
doubleclick.net	15.1KB	00:00	3	0	3
kontera.com	6,391B	00:06	2	0	2
addthis.com	1,365B	00:00	1	0	1
addthiscdn.com	1,231B	00:00	1	0	1
quantserve.com	1,847B	00:00	1	0	1
yandex.ru	2,021B	00:00	1	0	1

Find Domain or IP

Columns... | Export...

Applications Matched

No data was found in the selected time range

Malware Threats Detected

No data was found in the selected time range

Policies Matched

Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions
DefaultGroup	Access	568.6KB	118	0	118
NONE	Access	0B	0	5	5
Totals (all available data):	--	568.6KB	118	5	123

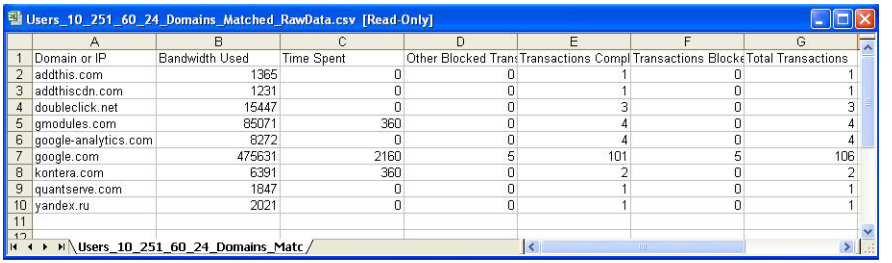
ユーザの詳細ページから総トランザクション別の URL カテゴリ、総トランザクション別のトレンド、一致する URL カテゴリ、一致するドメイン、一致するアプリケーション、検出されたマルウェアの脅威、および一致するポリシーを確認できます。

これらのカテゴリによって、10.251.60.24 のユーザがブロックされている URL（ページの [Domains] セクションに含まれる [Transactions Blocked] カラムに表示）にアクセスしようとしていたことなどがわかります。

ステップ 4　[Domains Matched] テーブルで [Export] をクリックすると、ユーザがアクセスしようとしたドメインと URL の完全なリストが表示されます。

図 D-1 に、ユーザからエクスポートされた情報のリストを示します。

図 D-1　　エクスポート データの例



	A	B	C	D	E	F	G
1	Domain or IP	Bandwidth Used	Time Spent	Other Blocked Trans	Transactions Compl	Transactions Blocke	Total Transactions
2	addthis.com	1365	0	0	1	0	1
3	addthiscdn.com	1231	0	0	1	0	1
4	doubleclick.net	15447	0	0	3	0	3
5	gmodules.com	85071	360	0	4	0	4
6	google-analytics.com	8272	0	0	4	0	4
7	google.com	475631	2160	5	101	5	106
8	kontera.com	6391	360	0	2	0	2
9	quantserve.com	1847	0	0	1	0	1
10	yandex.ru	2021	0	0	1	0	1
11							

ここから Web トラッキング機能を使用して、この特定のユーザの Web 使用状況をトラッキングし、表示することができます。

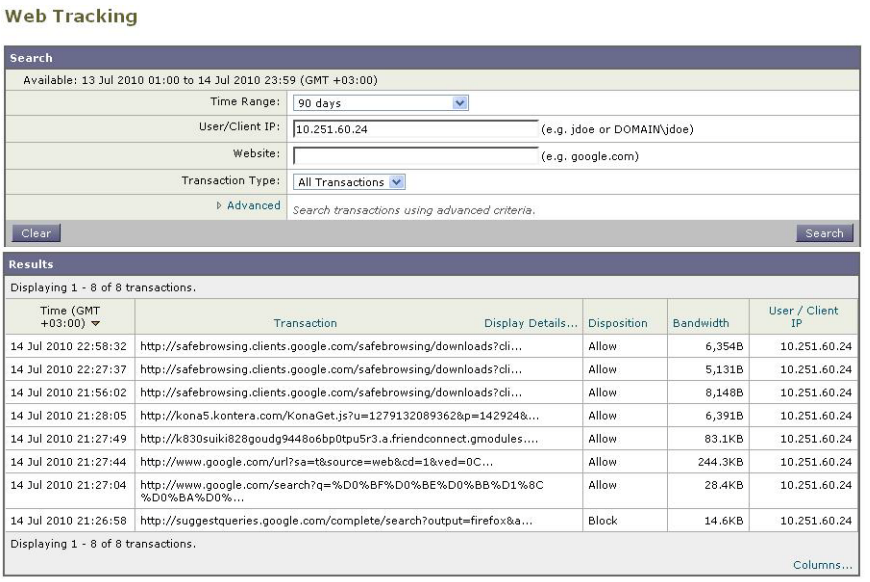
（注）　Web レポーティングでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Web Tracking] ページを使用します。

ステップ 5　[Web] > [Reporting] > [Web Tracking] を選択します。

ステップ 6　[User/Client IP Address] テキスト フィールドにユーザ名または IP アドレスを入力します。

この例では、10.251.60.24 のユーザの Web トラッキング情報を検索しています。

[Web Tracking] ページが表示されます。



このページから、10.251.60.24 のユーザがアクセスしたトランザクションの詳細なリストと URL を確認できます。

関連項目

表 D-1 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-1　　ユーザの調査の関連項目

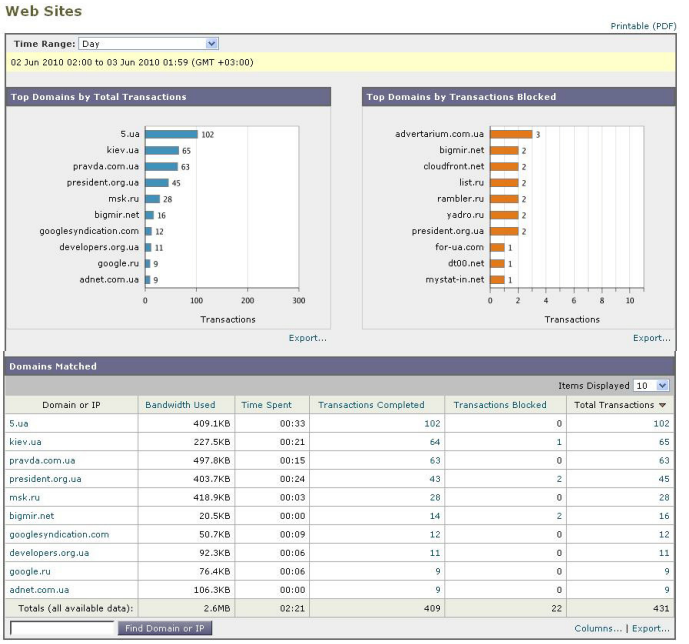
機能名	機能情報
[User] ページ	「[Users] ページ」（P.5-16）
[User Details] ページ	「[User Details] ページ」（P.5-20）
レポート データのエクスポート	「レポート データの印刷とエクスポート」（P.3-21）
Web トラッキング	「[Web Tracking] ページ」（P.5-70）

例 2：URL のトラッキング

このシナリオでは、セールス マネージャが、会社のサイトへのアクセスで、先週の上位 5 位を知りたい場合を考えます。さらに、どのユーザがこれらの Web サイトにアクセスしているかについても知りたいとします。

ステップ 1　Security Management アプライアンスで、[Web] > [Reporting] > [Web Sites] を選択します。

[Web Sites] ページが表示されます。



ステップ 2　[Time Range] ドロップダウン リストから [Week] を選択します。

ステップ 3　[Domains] セクションをスクロール ダウンすると、アクセスされているドメインまたは Web サイトが表示されます。

アクセス上位 25 位までの Web サイトは、[Domains Matched] テーブルに表示されます。同じテーブルで [Domain] または [IP] カラムのリンクをクリックすると、特定のアドレスまたはユーザが参照した実際の Web サイトを確認できます。

関連項目

表 D-2 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-2　URL のトラッキングの関連項目

機能名	機能情報
[Web Sites] ページ	「[Web Sites] ページ」（P.5-24）

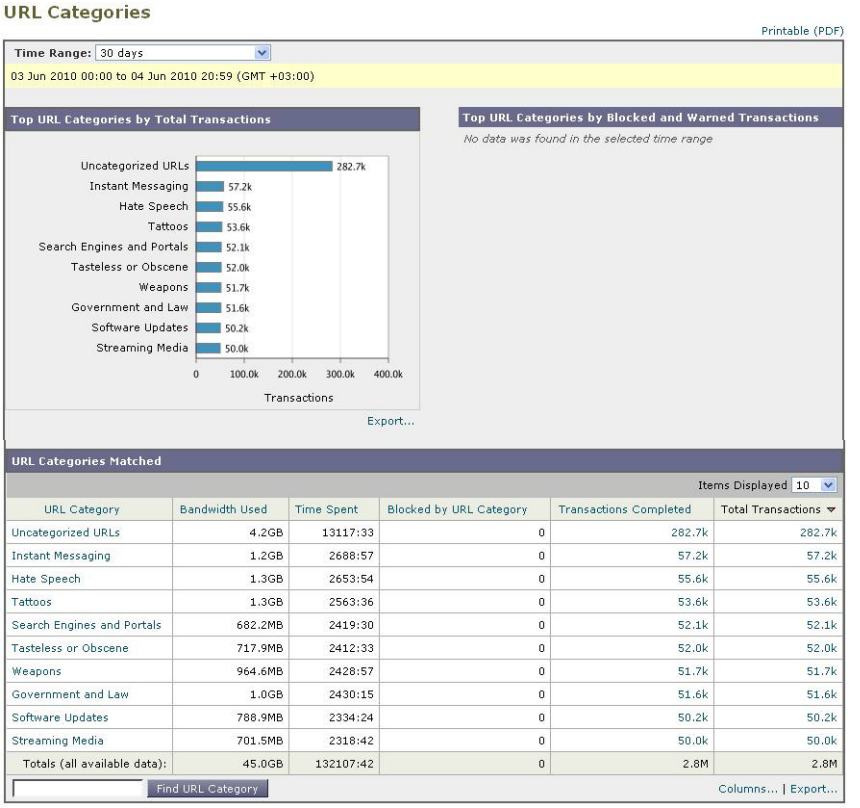
例 3：アクセスの多い URL カテゴリの調査

このシナリオでは、従業員が最近 30 日間にアクセスした上位 3 位までの URL を、人事部長が知りたい場合を考えます。また、ネットワーク管理者が、帯域幅の使用上をモニタしたり、ネットワークで最も帯域幅を使用している URL を特定したりするためにこの情報を取得するとします。

次の例は、複数の観点を持つ複数の人のためにデータを収集するが、生成するレポートは 1 つだけで済む方法を示します。

ステップ 1　Security Management アプライアンスで、[Web] > [Reporting] > [URL Categories] を選択します。

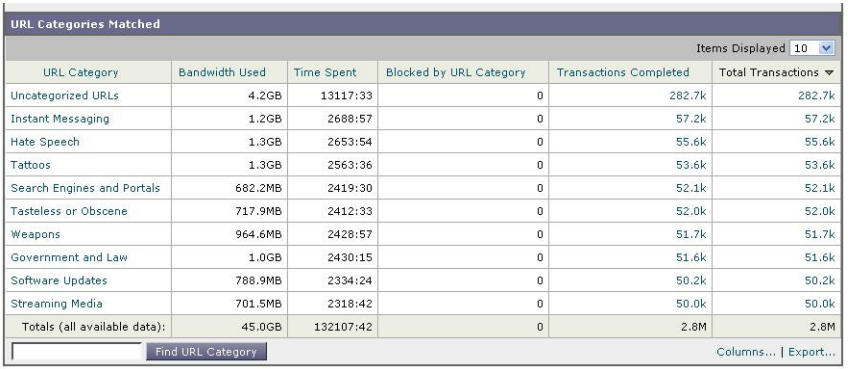
[URL Categories] ページが表示されます。



この例の [URL Categories] ページによると、総トランザクション別の上位 10 の URL カテゴリ グラフから、Instant Messaging、Hate Speech、Tattoo サイトなどの他に、282 k の未分類の URL にアクセスしていることがわかります。

ここで、[Export] リンクをクリックして未加工のデータを Excel スプレッドシートにエクスポートすると、このファイルを人事部長に送信できます。ネットワーク マネージャに URL ごとの帯域幅の使用量を知らせる必要があります。

ステップ 2　[URL Categories Matched] テーブルをスクロールダウンし、[Bandwidth Used] カラムを表示します。



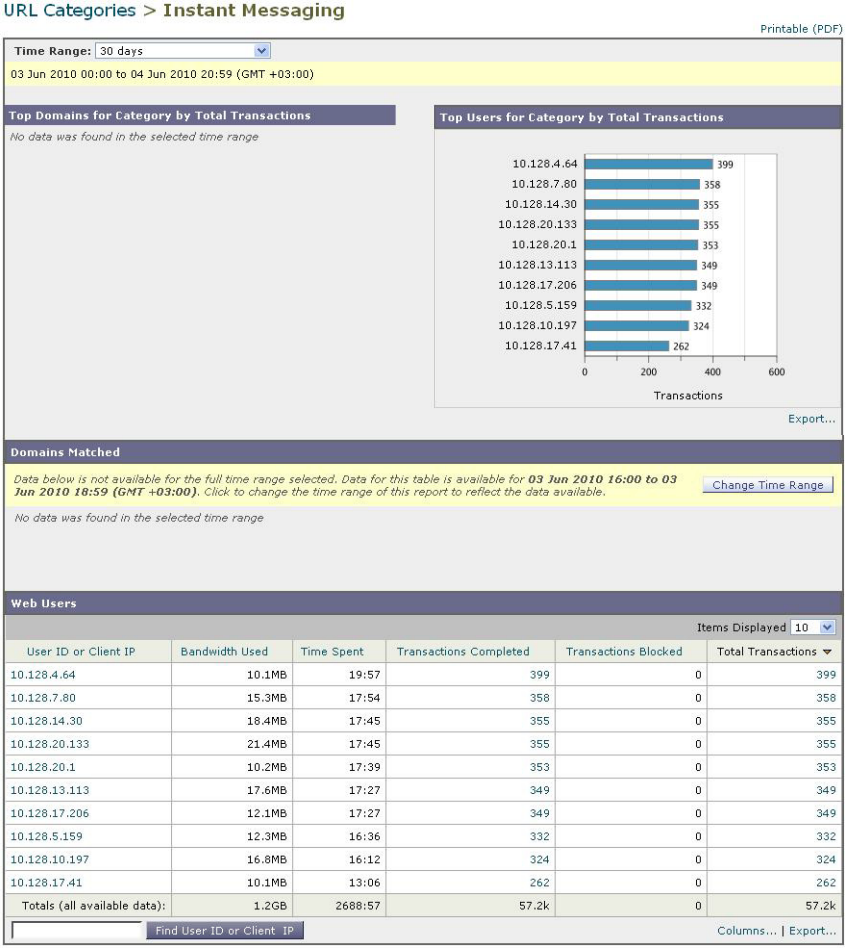
URL Categories Matched

Items Displayed 10

URL Category	Bandwidth Used	Time Spent	Blocked by URL Category	Transactions Completed	Total Transactions
Uncategorized URLs	4.2GB	13117:33	0	282.7k	282.7k
Instant Messaging	1.2GB	2688:57	0	57.2k	57.2k
Hate Speech	1.3GB	2653:54	0	55.6k	55.6k
Tattoos	1.3GB	2563:36	0	53.6k	53.6k
Search Engines and Portals	682.2MB	2419:30	0	52.1k	52.1k
Tasteless or Obscene	717.9MB	2412:33	0	52.0k	52.0k
Weapons	964.6MB	2428:57	0	51.7k	51.7k
Government and Law	1.0GB	2430:15	0	51.6k	51.6k
Software Updates	788.9MB	2334:24	0	50.2k	50.2k
Streaming Media	701.5MB	2318:42	0	50.0k	50.0k
Totals (all available data):	45.0GB	132107:42	0	2.8M	2.8M

Find URL Category　　Columns... | Export...

[URL Categories Matched] テーブルで、すべての URL カテゴリの帯域幅の使用量を確認することができます。もう一度 [Export] リンクをクリックして、このファイルをネットワーク管理者に送信します。さらに細かく調べるには、[Instant Messaging] リンクをクリックすると、どのユーザが帯域幅を大量に使用しているかが特定されます。次のページが表示されます。



このページから、ネットワーク管理者が Instant Messaging サイトの上位 10 ユーザを知ることができます。

このページから、最近 30 日間で 10.128.4.64 のユーザが Instant Messaging サイトに 19 時間 57 分アクセスしており、この期間の帯域幅の使用量が 10.1 MB であることがわかります。

関連項目

表 D-3 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-3　アクセスの多い URL カテゴリの調査の関連項目

機能名	機能情報
[URL Categories] ページ	「[URL Categories] ページ」（P.5-28）
レポート データのエクスポート	「レポート データの印刷とエクスポート」（P.3-21）

例 4：プライバシーおよびユーザ名の非表示

この例では、マネージャが一連のレポートを作成するが、従業員の個人情報は一切表示しない場合を考えます。

Security Management アプライアンスでは、[Reports] チェックボックスの [Anonymize User Names] をクリックすると、この操作をイネーブルまたはディセーブルにできます。この操作をイネーブルにすると、レポートを受け取った人にユーザ名を明らかにすることなく、レポートを生成して配布することができます。

次の例は、ユーザ名や IP アドレスなどの個人情報がレポートにどのように表示されるのか、およびユーザ名を匿名にするとどのようなレポートになるのかを示しています。

ユーザ名の匿名化のイネーブル化前

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

[Centralized Web Reporting] ページが表示されます。

（注）　システム セットアップ ウィザードを実行してから初めて中央集中型レポーティングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[Accept] をクリックします。「中央集中型 Web レポーティングの設定」（P.5-3）を参照してください。

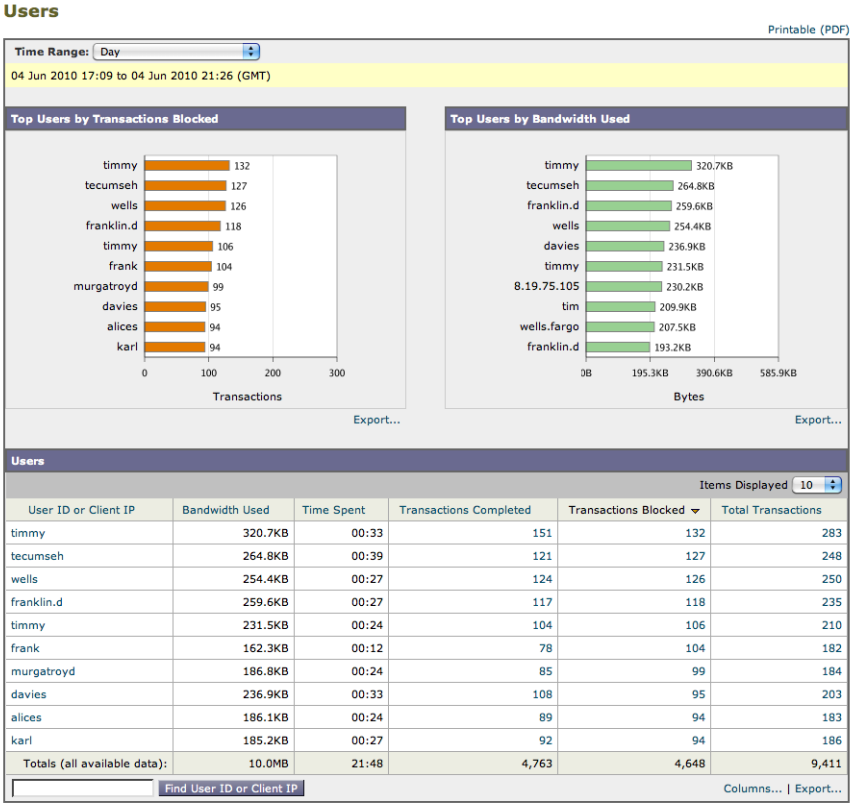
ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Anonymize User Names in Report] チェックボックスがオフになっていることを確認してください。

ステップ 4　[Submit] をクリックします。

ステップ 5　[Web] > [Users] を選択します。

ステップ 6　[Web Users] ページが表示されます。



この場合は、すべてのユーザ名が [Web] > [Users] ページに表示されます。

ユーザ名を確認したい場合は、この情報が表示されていても問題ありません。それに対して、この情報を他のグループに公開しない場合は、ユーザ名を非表示にする必要があります。

（注）　管理者ステータスを持っている場合は、常にユーザ名が表示されます。

ユーザ名の匿名化のイネーブル化後

レポート機能でユーザ名の匿名化を使用すると、同じレポートが次のようになります。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

[Centralized Web Reporting] ページが表示されます。

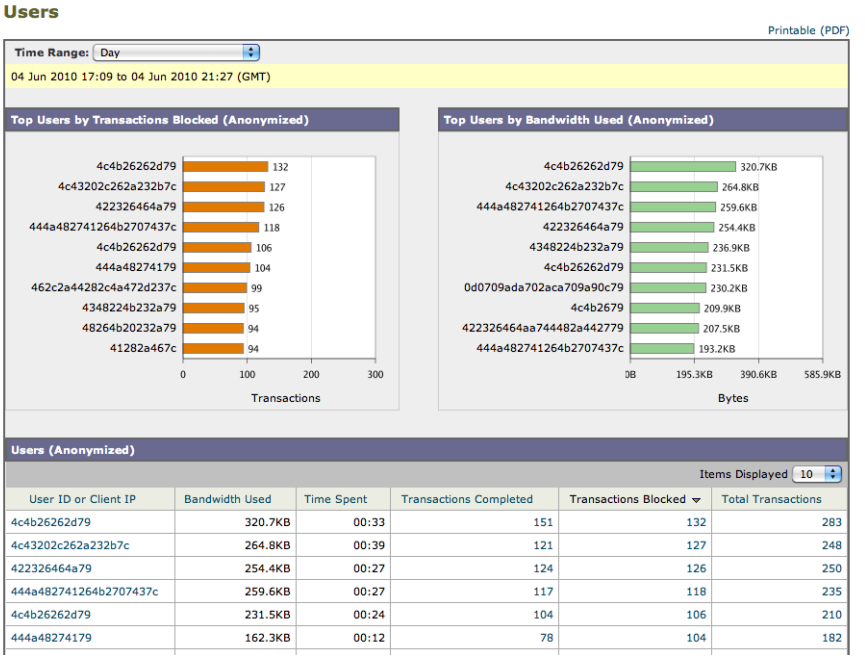
ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Anonymize User Names in Report] チェックボックスをオンにします。

ステップ 4　[Submit] をクリックします。

ステップ 5　[Web] > [Users] を選択します。

ステップ 6　[Web Users] ページが表示されます。



この場合は、ユーザ名が [Web] > [Users] ページに表示されません。

関連項目

表 D-4 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-4　プライバシー情報の関連項目

機能名	機能情報
Web レポーティング	「Web レポーティングを使用する前に」（P.5-3）
Web レポーティングのイネーブル化	「中央集中型 Web レポーティングの設定」（P.5-3）
[User] ページ	「[Users] ページ」（P.5-16）

例 5：既存の Security Management アプライアンスでの新しい Configuration Master へのアップグレード

（注）　この例は、Configuration 6.3 を初期化済みであることを前提としています。

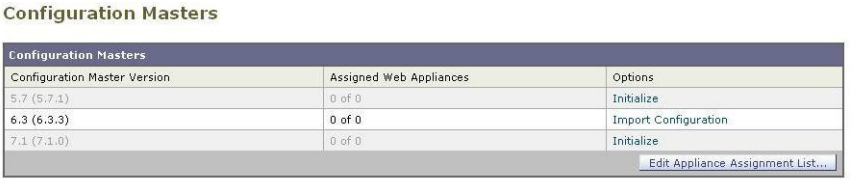
ここでは、既存の Security Management アプライアンスを新しい Configuration Master にアップグレードする方法について説明します。

この例では、ユーザが Configuration Master 6.3 を実行している既存の Security Management アプライアンスを Configuration Master 7.1 にアップグレードする場合を考えます。

アップグレードを行う手順は、次のとおりです。

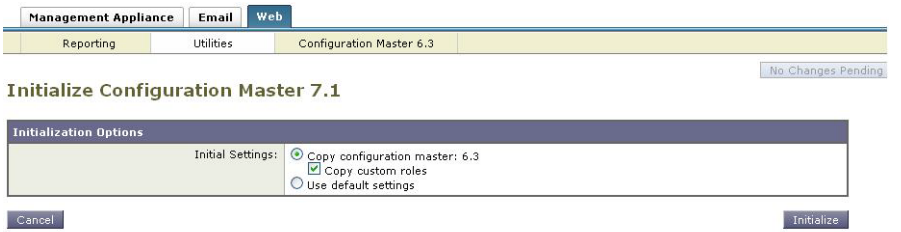
ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

[Configuration Masters] ページが表示されます。



このページから、Configuration Master 6.3 がすでに初期化されていることと、Configuration Master 7.1 が初期化されていないことがわかります。また、唯一の Configuration Master（Configuration Master 6.3）が Security Management アプライアンスのタブの下に表示されていることも確認できます。

ステップ 2　7.1 の行で [Initialize] をクリックします。



ステップ 3　[Copy Configuration Master 6.3] オプション ボタンをクリックし、[Copy custom rules] チェックボックスをオンにします。

[Copying the custom rules] チェックボックスをオンにすると、現在 Configuration Master 6.3 に設定しているユーザ ロールまたは固有のポリシーを維持したまま、新規の Configuration Master 7.1 にデータを転送することができます。

ステップ 4　[Initialize] をクリックします。

Configuration Master 7.1 が初期化され、使用できるようになりました。

関連項目

表 D-5 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-5　新しい Configuration Master のアップグレードの関連項目

機能名	機能情報
Configuration Master	「Configuration Master の操作」（P.8-3）

例 6：既存の Web セキュリティ アプライアンスからのコンフィギュレーション ファイルのインポート

（注）　この例は、Configuration 6.3 を初期化済みであることを前提としています。

この例では、Web セキュリティ アプライアンスから既存のコンフィギュレーションを、既存の Security Management アプライアンスにインポートする方法について説明します。

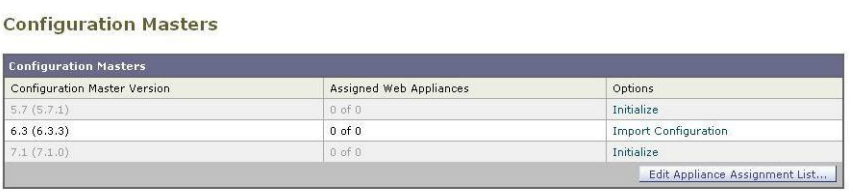
このシナリオでは、ユーザのすべての Web セキュリティ アプライアンスで中央集中型コンフィギュレーション管理を使用することを、ユーザが決定しています。これを行うため、ユーザは最近 Security Management アプライアンスを購入し、Web セキュリティ アプライアンスのすべての管理を行います。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Centralized Configuration Manager] を選択します。

ステップ 2　[Enable] をクリックします。

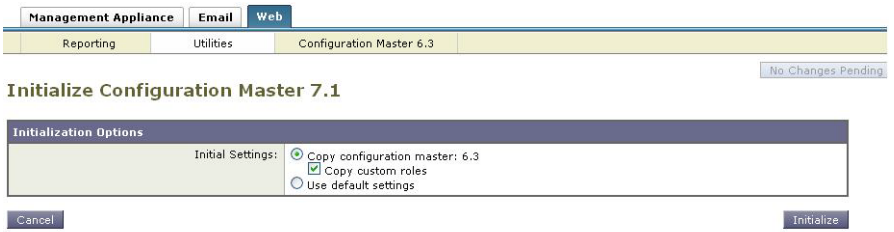
ステップ 3　[Web] > [Utilities] > [Configuration Masters] の順にクリックします。

[Configuration Masters] ページが表示されます。



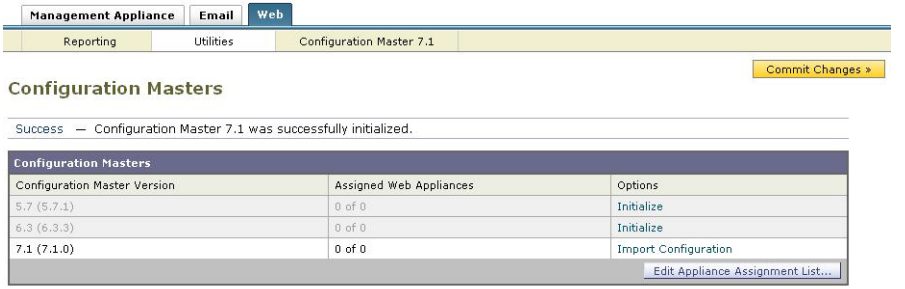
このページから、Configuration Master 6.3 がすでに初期化されていることと、Configuration Master 7.1 が初期化されていないことがわかります。また、唯一の Configuration Master（Configuration Master 6.3）が Security Management アプライアンスのタブの下に表示されていることも確認できます。

ステップ 4　7.1 の行で [Initialize] をクリックします。



ステップ 5　[Use Default Settings] オプション ボタンをクリックします。

[Configuration Masters] ページが表示され、初期化が成功したが示されます。



ステップ 6　[Import Configuration] をクリックします。

[Import Web Configuration] ページが表示されます。

ステップ 7　[Select Configuration Source] ドロップダウン メニューから [Web Configuration File] を選択します。

ステップ 8　[Load a Valid Configuration File from a Web Security Appliance] の横にあるテキスト フィールドで [Browse] をクリックし、Web セキュリティ アプライアンスからインポートする有効な XML ファイルを選択します。

ステップ 9　[Import] をクリックします。

選択した XML ファイルが Web セキュリティ アプライアンスからロードされます。

ステップ 10　[Confirm Import] をクリックします。

その他の考慮事項

Security Management アプライアンスに ID を作成する際には、特定のアプライアンスのみに適用されるオプションが用意されています。たとえば、Security Management アプライアンスを購入し、Web セキュリティ アプライアンスごとに作成された既存の Web セキュリティ アプライアンス コンフィギュレーションとポリシーを保持する場合は、1 つのファイルをマシンにロードし、次に他のマシンから手動でポリシーを追加する必要があります。

これを実行するための方法の 1 つとして、各アプライアンスに一連の ID を作成し、これらの ID を参照するポリシーを設定する方法があります。Security Management アプライアンスがコンフィギュレーションを公開すると、これらの ID と、ID を参照するポリシーは、自動的に削除され、ディセーブルになります。この方法を使用すると、手動で何も設定する必要がありません。これは基本的に「アプライアンスごとの」ID です。

この方法では、デフォルトのポリシーまたは ID が、サイト間で異なる場合だけが問題となります。たとえば、あるサイトではポリシーを「default allow with auth」に設定し、別のサイトでは「default deny」に設定している場合です。この場合、アプライアンスごとの ID とポリシーをデフォルトのすぐ上に作成する必要があります。基本的には独自の「デフォルト」のポリシーを作成します。

関連項目

表 D-6 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-6　新しいコンフィギュレーション ファイルのインポートの関連項目

機能名	機能情報
Configuration Master	「Configuration Master の操作」（P.8-3）

例 7：リモート Web セキュリティ アプライアンスでのアクセス ポリシーのカスタマイズと、中央 Security Management アプライアンスでの管理

（注）　この例は、Configuration 6.3 を初期化済みであることを前提としています。

多くの顧客は、1 つの Security Management アプライアンスを使用して複数の Web セキュリティ アプライアンスの導入環境を管理したいと考えています。その場合、現地法が異なるため、地理的なロケーションによってアクセス ポリシーが変わる可能性があります。

たとえば、中国、北米、およびヨーロッパの従業員向けにカスタマイズされた一連のルールが必要なことがあります。ここでは、アクセス ポリシーはローカルに管理できます。

このシナリオでは、地理的にリモートの Web セキュリティ アプライアンス向けにアクセス ポリシーをカスタマイズし、Security Management アプライアンスのローカル管理者にアクセス ポリシーのローカル制御を許可する方法を説明します。

このシナリオでは、ID を作成して 3 つのロケーションそれぞれでユーザを識別し、その後そのロケーション向けに適切なアクセス ポリシーを作成します。次に、ロケーションの ID を、カスタマイズされたロケーションのアクセス ポリシーに追加する必要があります。ユーザがこの ID にタグ付けを行うと、この ID の一部であるポリシーが、ユーザのこのセットに適用されます。最後に、ローカルなアクセス ポリシーを維持するための委任管理者を作成する必要があります。

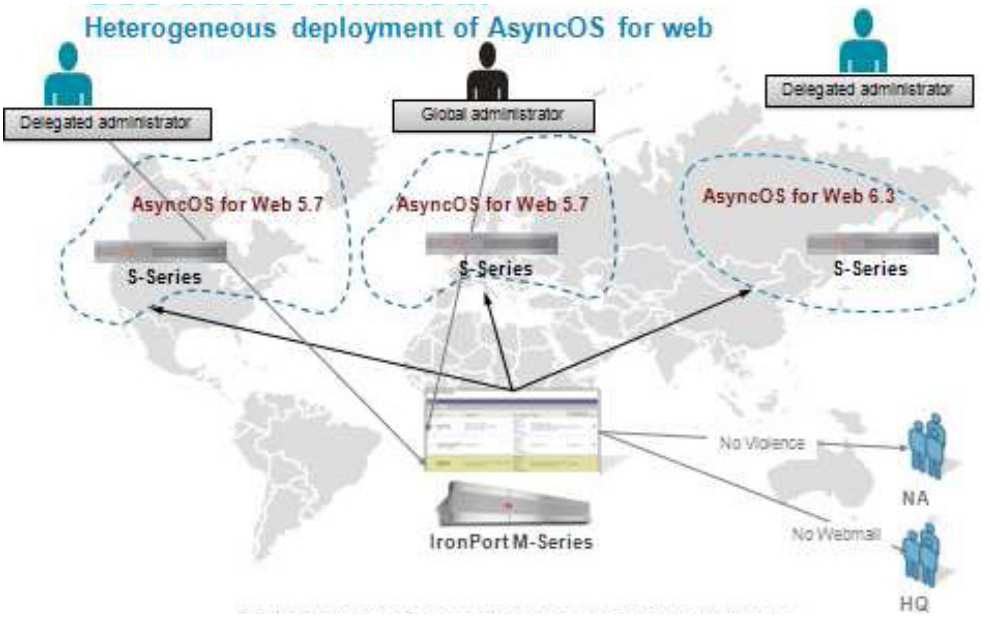
これを行うには、次の手順を実行します。

	アクション	説明
ステップ 1	アクセス ルールの設定	この例では、3 つのアクセス ルールを設定し、必要に応じてこれらのルールをアクセス ポリシーに組み込みます。 • ソーシャル ネットワーク アクセスのルールにより、ソーシャル ネットワークのサイトに対するアクセスが制限されます。 • 武器および暴力のアクセス ルールにより、武器のサイトと暴力のサイトに対するアクセスが制限されます。 • Web ベースの電子メール アクセス ルールにより、Web ベースの電子メールへのアクセスが制限されます。
ステップ 2	アクセス ルールの適用先の決定	ソーシャル ネットワーク アクセスのルールは、すべてのサイトに適用されます。可能であれば、このルールをグローバル アクセス ポリシーに組み込みます。 武器および暴力のルールは、北米（NA）のサイトに適用されます。このルールを NA アクセス ポリシーに組み込みます。Web ベースの電子メール アクセス ルールは、ヨーロッパの本社サイトに適用されます。このルールを HQ アクセス ポリシーに組み込みます。
ステップ 3	ID の作成	この手順により、ポリシーが適用されるユーザの ID と、このユーザが使用する Web セキュリティ アプライアンスの ID を作成できます。 個々のサイトは対応する Web セキュリティ アプライアンスと、ユーザが接続するサブネットによって識別されます。

	アクション	説明
ステップ 4	Configuration Master 5.7 用のカスタム URL カテゴリの作成	AsyncOS 5.7 にはソーシャル ネットワーク URL カテゴリがなく、6.3 には存在するため、AsyncOS 5.7 および 6.3 を実行する Web セキュリティ アプライアンス全体でポリシーを統一するため、カスタム URL カテゴリを作成する必要があります。
ステップ 5	アクセス ポリシーの作成と ID の追加	グローバル ポリシーでは、ソーシャル ネットワーク サイトへのアクセスが禁止されます。北米のアクセス ポリシーでは、武器および暴力サイトへのアクセスが禁止されます。ヨーロッパのアクセス ポリシーでは、Web ベースの電子メールへのアクセスが禁止されます。 さらに、アクセス ポリシーが適用されるユーザを指定する ID と、このポリシーが適用されるサイトを指定するカスタム URL カテゴリを追加する必要があります。
ステップ 6	委任管理者の作成	北米とヨーロッパ向けのローカル アクセス ポリシーは、ローカル ポリシーおよびローカル ルールに詳しい管理者により、ローカル サイトで維持されます。

図 D-2 に、この委任がどのように機能するかを示します。

図 D-2　委任管理



アクセス ルールの設定

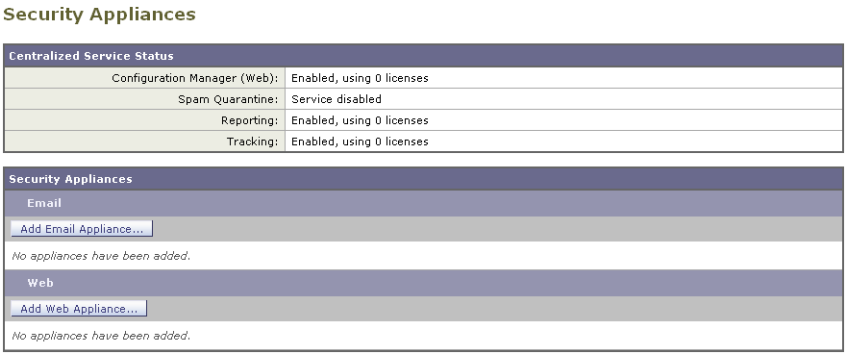
この例では、3 つのアクセス ルールを設定し、必要に応じてこれらのルールをアクセス ポリシーに組み込みます。

- ソーシャル ネットワーク アクセスのルールにより、ソーシャル ネットワークのサイトに対するアクセスが制限されます。
- 武器および暴力のアクセス ルールにより、武器のサイトと暴力のサイトに対するアクセスが制限されます。
- Web ベースの電子メール アクセス ルールにより、Web ベースの電子メールへのアクセスが制限されます。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

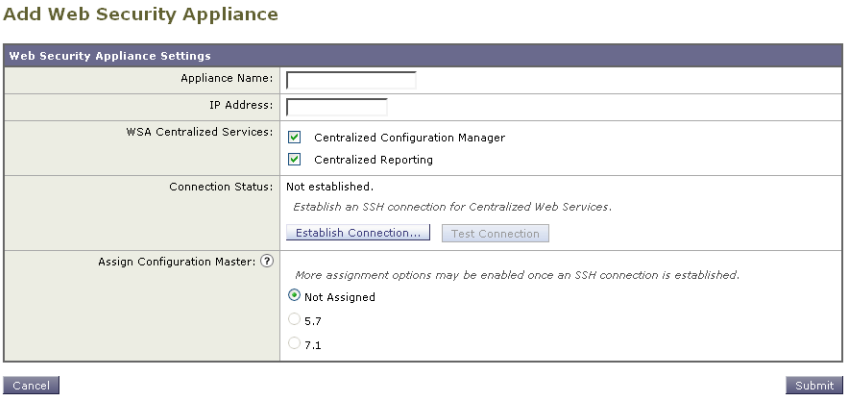
[Security Appliances] ページが表示されます。

図 D-3　[Security Appliances] ページ



ステップ 2　[Add Web Appliance] ボタンをクリックして、[Add Web Security Appliance] ページを表示します

図 D-4　[Add Web Security Appliance] ページ



ステップ 3　[Appliance Name] テキスト フィールドおよび [IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

この例では、アプライアンス名は、China、HQ および NA です。

（注）　[IP Address] テキスト フィールドに DNS 名を入力した場合でも、[Submit] をクリックすると、すぐに IP アドレスに解決されます。

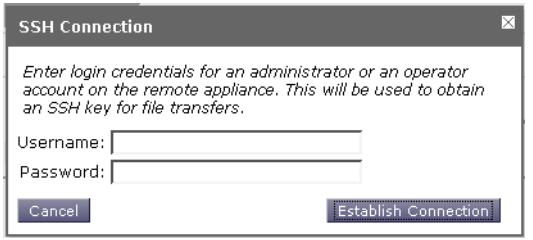
ステップ 4　Cisco IronPort アプライアンスを管理する際に使用するサービスを選択します。

（注）　Security Management アプライアンスでイネーブルにしたサービスのみ選択できます。

ステップ 5　[Establish Connection] をクリックします。

[SSH Connection] ダイアログボックスが表示されます。

図 D-5　[SSH Connection] ダイアログボックス



ステップ 6　[Username] および [Password] テキスト フィールドに、Cisco IronPort アプライアンス上の管理者アカウントのログイン資格情報を入力します。

（注）　ログイン資格情報を入力すると、Security Management アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、Security Management アプライアンスには保存されません。

ステップ 7　[Establish Connection] をクリックして、モニタリング サービス用の接続を確立します。

ステップ 8　[Test Connection] をクリックして、リモート アプライアンスのモニタリング サービスが正しく設定され、互換性があることを確認します。

ステップ 9　Web セキュリティ アプライアンスを追加する場合は、アプライアンスを割り当てる Configuration Master を選択します。

各 Configuration Master には、Web セキュリティ アプライアンスのバージョンごとの設定が含まれています。Security Management アプライアンスは、互換性のある AsyncOS のバージョンを実行する Web セキュリティ アプライアンスにのみ Configuration Master を公開できます（たとえば、Web セキュリティ アプライアンスが AsyncOS 6.3 を実行している場合、Configuration Master として

6.3.0 を選択します）。[Web] > [Utilities] > [Configuration Masters] を選択して、後で Web セキュリティ アプライアンスを割り当てることもできます（「Web セキュリティ アプライアンスと Configuration Master の関連付け」（P.8）を参照）。

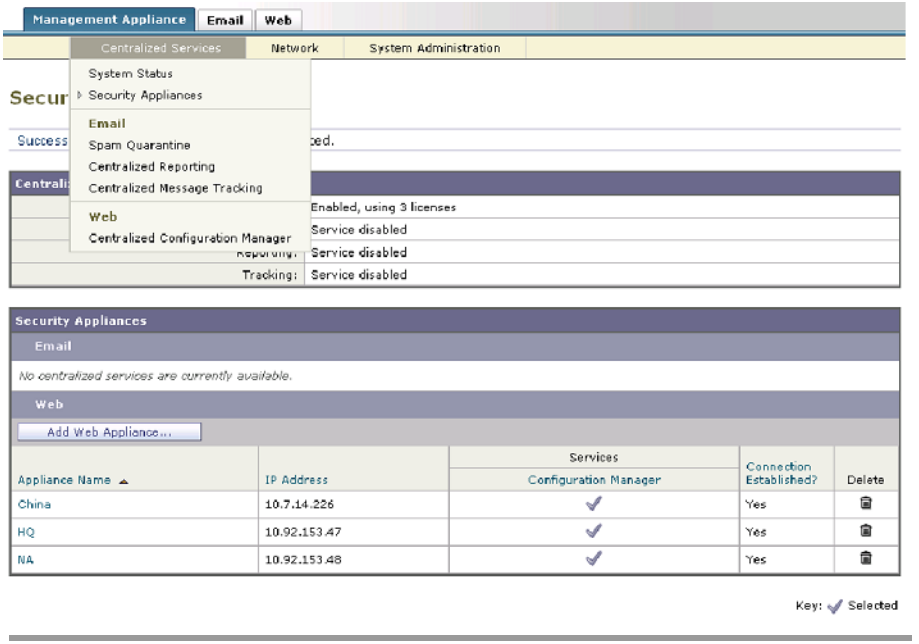
Configuration Master および Web セキュリティ アプライアンスの管理の詳細については、第 8 章「Web セキュリティ アプライアンスの管理」を参照してください。

ステップ 10　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

[Security Appliances] ページには、追加した管理対象アプライアンスが表示されます。チェック マークは、イネーブルになっているサービスを示し、[Connection Established?] カラムは、モニタリング サービスの接続が適切に設定されているかどうかを示します。

図 D-6 に、新たに追加された管理対象のアプライアンスが表示されます。

図 D-6　委任管理用に追加された Web セキュリティ アプライアンス



アクセス ルールの適用先の決定

この手順では、社内の全員に適用される次のグローバルなアクセス ポリシーを定義します。

- ソーシャル ネットワーク ルール

  このアクセス ポリシーはすべてのサイトに適用されます。

- 武器および暴力ルール

  このポリシーは北米拠点へローカルに適用されます。

- Web ベースの電子メール ルール

  このポリシーは HQ 拠点へローカルに適用されます。

（注） アクセス ポリシーの設定を開始する前に、中央集中型 Web コンフィギュレーション マネージャがイネーブルになっていることを確認します。

ステップ 1 Security Management アプライアンスで、[Web] > [Configuration Manager 7.1] > [Access Policies] を選択します。

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [Access Policy:Add Group] ウィンドウで、[Social Networking Rule] と入力し、このポリシーをすべてのサイトに適用します。

ステップ 4 [Submit] をクリックします。

ステップ 5 [Web] > [Configuration Manager 7.1] > [Access Policies] に戻り、[Add Policy] をクリックします。

ステップ 6 [Access Policy:Add Group] ウィンドウで、[Weapons and Violence Rule] と入力し、このポリシーを北米のサイトに適用します。

ステップ 7 [Submit] をクリックします。

ステップ 8 最後に、[Web] > [Configuration Manager 7.1] > [Access Policies] に戻り、[Add Policy] をクリックします。

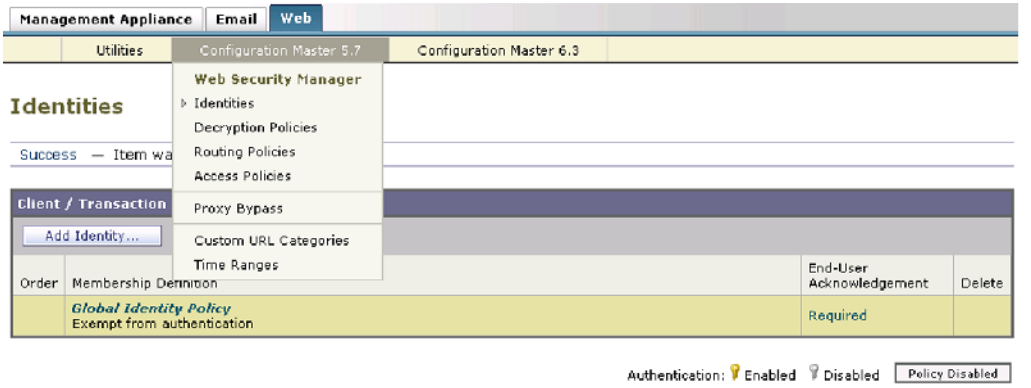
ステップ 9 [Access Policy:Add Group] ウィンドウで、[Web-based Email Rule] と入力し、このポリシーを HQ サイトに適用します。

ステップ 10 [Submit] をクリックします。

ID の作成

この手順により、ポリシーが適用されるユーザの ID と、このユーザが使用する Web セキュリティ アプライアンスの ID を作成できます。個々のサイトは対応する Web セキュリティ アプライアンスと、ユーザが接続するサブネットによって識別されます。

ステップ 1　[Web] > [Configuration Master 5.7] > [Identities] > [Add Identities] を選択し、中国拠点の ID を作成します。

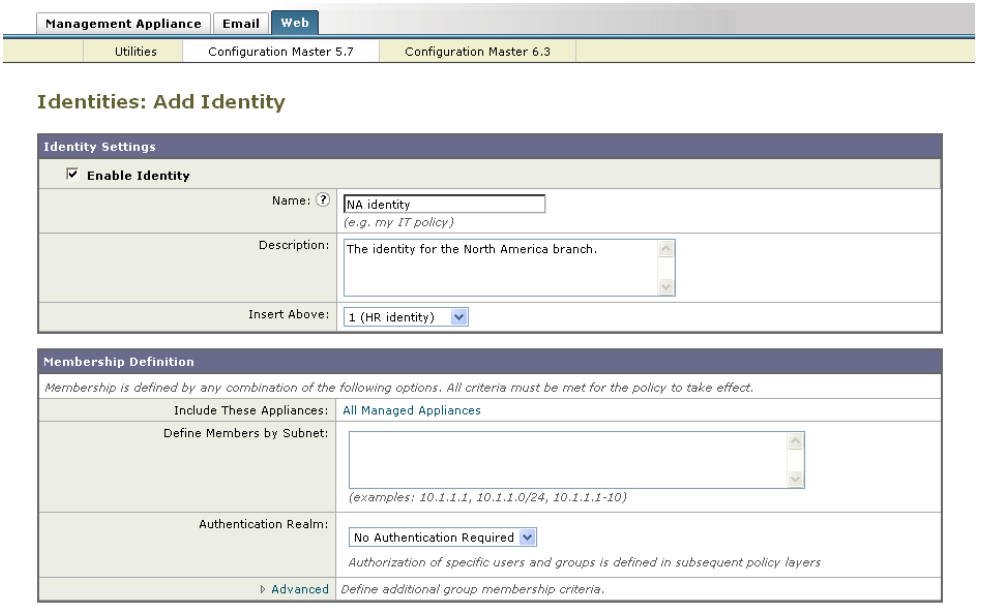


ステップ 2　[Web] > [Configuration Master 5.7] > [Identities] > [Add Identities] を選択し、北米拠点の ID を作成します。

武器および暴力ルールは、北米のサイトだけに適用されます。北米サイトの Web セキュリティ アプライアンスは AsyncOS 5.7 を実行しています。

ステップ 3　[Identity Settings] テキスト フィールドで、[NA identity] と入力します。

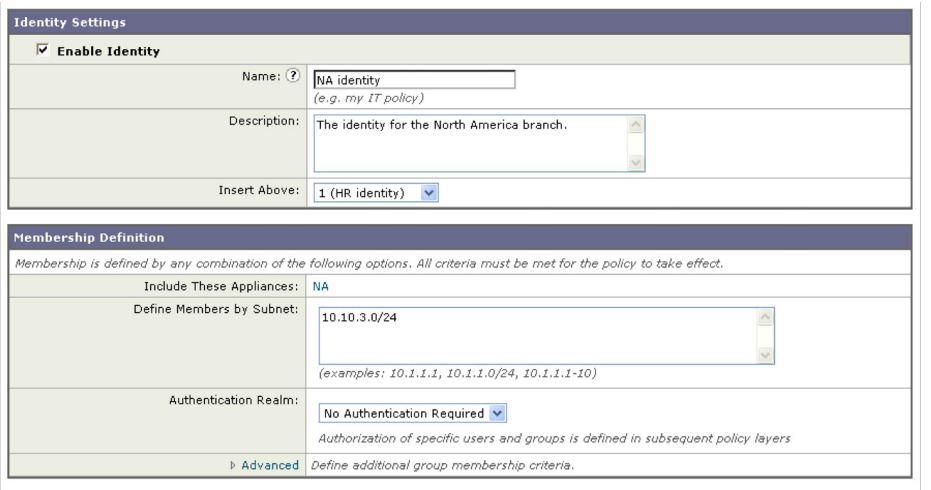
ステップ 4　[Include these Appliances] の横にある [All Managed Appliances] をクリックして、北米サイトのアプライアンスに ID を制限します。



ステップ 5　[Web] > [Identity Policies] > [Managed Appliances] を選択します。

ステップ 6　[NA] の横にあるチェックボックスをオンにします。

この例では、ユーザのグループが 10.10.3.0/24 サブネット上にあります。

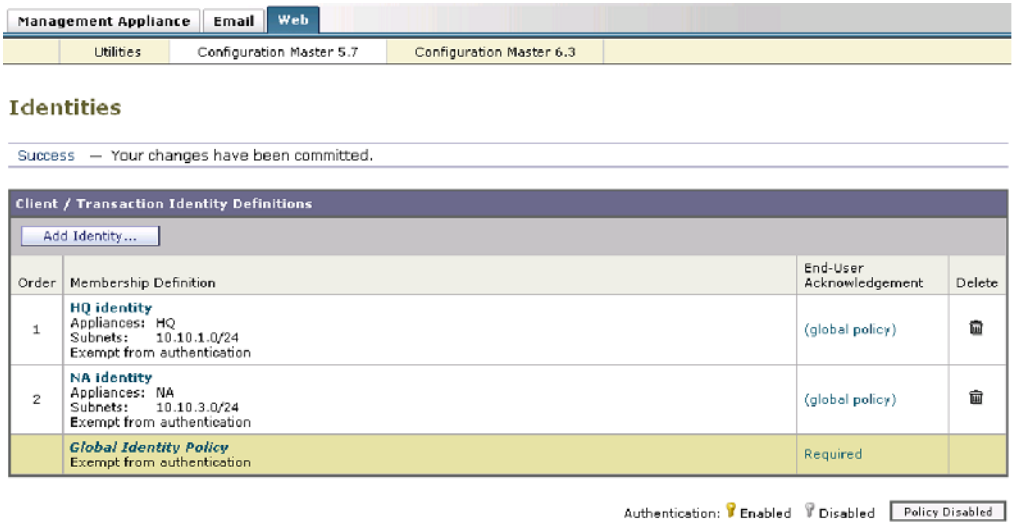


ステップ 7　NA に対して実行した手順（ステップ 2 ～ 6）と同じ手順で、**HQ** の ID を新たに作成します。

この ID の **HQ** Web セキュリティ アプライアンスのチェックボックスを選択します。この例のユーザのグループは 10.10.1.0/24 サブネット上にあります。

これで、図 D-7 に示すように 2 つの ID が作成されます。

図 D-7　作成された ID



Configuration Master 5.7 用のカスタム URL カテゴリの作成

AsyncOS 6.3 ではソーシャル ネットワーク URL カテゴリを使用できますが、AsyncOS 5.7 では使用できないため、カスタム URL カテゴリを作成する必要があります。

ソーシャル ネットワーク カスタム カテゴリには次のサイトが含まれます。

- myspace.com
- facebook.com
- linkedin.com

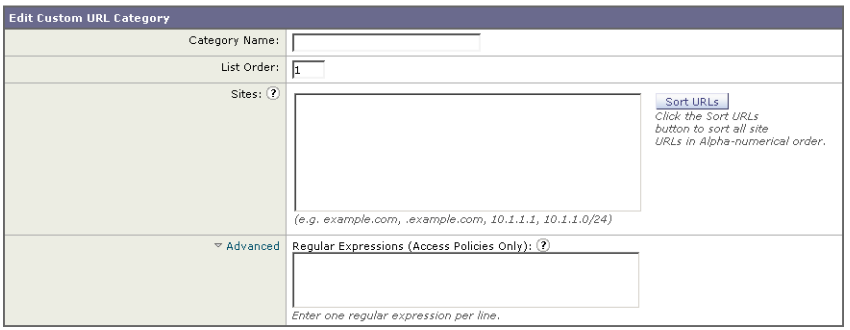
- twitter.com
- badoo.com

ステップ 1　Security Management アプライアンスで、[Web] > [Configuration Master 7.1] > [Custom URL Categories] を選択します。

[Custom URL Categories] ページが表示されます。

ステップ 2　[Add Custom Category] をクリックして、5.7 用のソーシャル ネットワークを作成します。

図 D-8　　カスタム URL カテゴリの作成

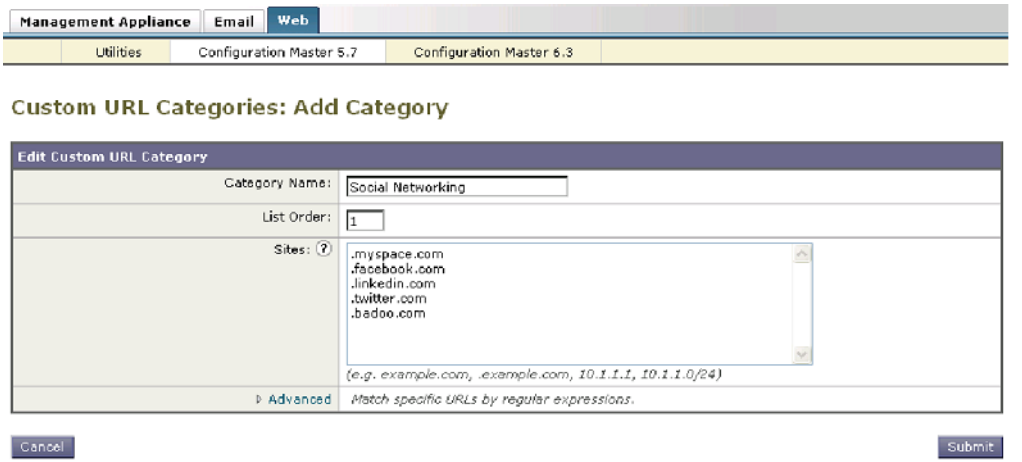


ステップ 3　カスタム URL カテゴリを作成または編集するには、次の設定を該当するフィールドに入力します。

- [Category Name] : URL カテゴリの名前を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。
- [Sites] : ソーシャル ネットワーク カテゴリに属するドメイン名を入力します。

  複数のアドレスは、改行またはカンマで区切って入力します。
  この例では、次のドメインを使用しています。
  - myspace.com
  - facebook.com
  - linkedin.com
  - twitter.com
  - badoo.com

図 D-9　　カスタム URL カテゴリ



ステップ 4　[Submit] をクリックしてページ上の変更を送信し、[Commit Changes] をクリックしてアプライアンスへの変更を確定します。

アクセス ポリシーの作成と ID の追加

この手順では、ソーシャル ネットワーク サイトへのアクセスを制限するすべてのサイト向けのアクセス ポリシーを作成します。次の 3 つのポリシーを作成する必要があります。

- China Policy
- NA policy
- HQ policy

中国拠点の Web セキュリティ アプライアンスは、Configuration Master 6.3 だけを実行しています。中国拠点に対する唯一のアクセス ポリシー ルールは、ソーシャル ネットワーク サイトへのアクセスを禁止するルールです。ソーシャル ネットワーク カテゴリは Configuration Master 6.3 の URL カテゴリのセットに含まれているため、ソーシャル ネットワークが、アクセスが禁止されている URL カテゴリとして選択されていることを確認する必要があります。

ステップ 1　Security Management アプライアンスで、[Web] > [Configuration Master 6.3] > [Access Policies] を選択します。

ステップ 2　[URL Categories] カラムのリンクをクリックし、グローバル アクセス ポリシーを変更します。

ステップ 3　[Social Networking] が選択され、割り当てられた ID がブロックされていることを確認します。

NA 拠点の Web セキュリティ アプライアンスは AsyncOS 5.7 を実行しています。NA アクセス ポリシーには、次の 2 つのルールを適用する必要があります。

- 武器および暴力サイトへのアクセスを禁止するローカル ルール。
- ソーシャル ネットワーク サイトへのアクセスを禁止するルール。

ソーシャル ネットワーク カテゴリは 5.7 に含まれていないため、ソーシャル ネットワークを確実に禁止するには、ソーシャル ネットワークのカスタム URL カテゴリを作成する必要があります。

ステップ 4　Security Management アプライアンスで、[Web] > [Configuration Master 5.7] > [Access Policies] を選択します。

ステップ 5　[Add Policy] をクリックします。

ステップ 6　[Access Policies: Add Policy] ページで次の手順を実行します。

- [Policy Setting] セクションで [Enable Policy] チェックボックスをオンにします。
- [Policy Name] テキスト フィールドに [NA policy] と入力します。
- [Policy Member Definition] セクションで、ドロップダウン リストから [NA Identity] を選択します。

ステップ 7　[Submit] をクリックします。

[Submit] をクリックすると、[Access Policies] ページに戻ります。

ステップ 8　[Access Policies] ページの NA アクセス ポリシー行で、[URL Categories] カラムの [global policy] リンクをクリックします。

ステップ 9　Weapons URL カテゴリおよび Violence URL カテゴリが、このアクセス ポリシーに選択されていることを確認します。さらに、[Social Networking] カスタム URL カテゴリがブロックされていることを確認します。

最後に HQ 拠点ポリシーを処理する必要があります。HQ 拠点の Web セキュリティ アプライアンスは AsyncOS 5.7 を実行しています。NA アクセス ポリシーには、次の 2 つのルールを適用する必要があります。

- Web ベースの電子メール サイトへのアクセスを禁止するローカル ルール。
- ソーシャル ネットワーク サイトへのアクセスを禁止するルール。

ソーシャル ネットワーク カテゴリは 5.7 に含まれていないため、ソーシャル ネットワークを確実に禁止するには、ソーシャル ネットワークのカスタム URL カテゴリを作成する必要があります。

ステップ 10　Security Management アプライアンスで、[Web] > [Configuration Master 5.7] > [Access Policies] を選択します。

ステップ 11　[Add Policy] をクリックします。

ステップ 12　[Access Policies: Add Policy] ページで次の手順を実行します。

- [Policy Setting] セクションで [Enable Policy] チェックボックスをオンにします。
- [Policy Name] テキスト フィールドに [HQpolicy] と入力します。
- [Policy Member Definition] セクションで、ドロップダウン リストから [HQ Identity] を選択します。

ステップ 13　[Submit] をクリックします。

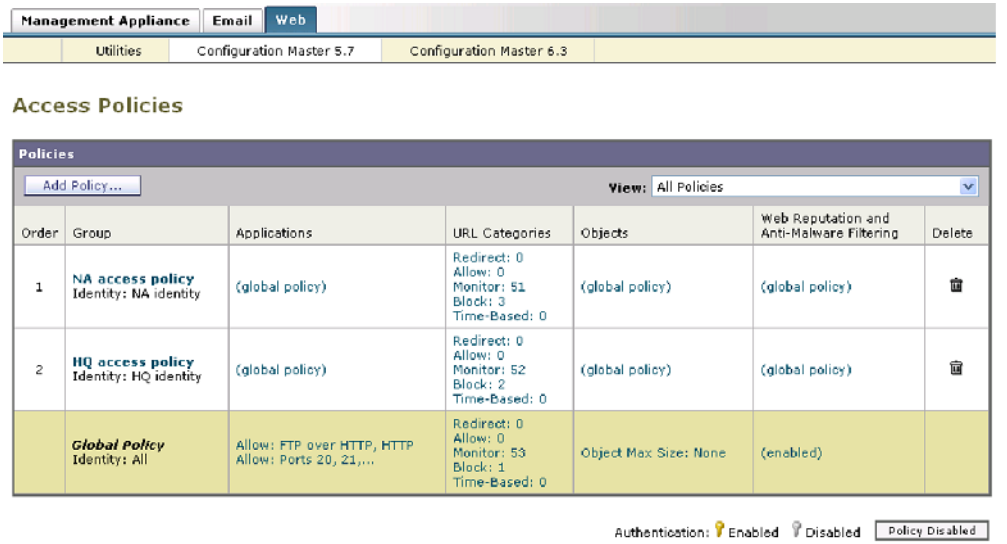
[Submit] をクリックすると、[Access Policies] ページに戻ります。

ステップ 14　[Access Policies] ページの HQ アクセス ポリシー行で、[URL Categories] カラムの [global policy] リンクをクリックします。

ステップ 15　[Social Networking] カスタム URL カテゴリがブロックされていることを確認します。さらに、[Web-based Email] カテゴリがブロックされていることを確認します。

これで、本社の Web セキュリティ アプライアンスにおけるデフォルトのソーシャル ネットワーク ポリシーが、新しいソーシャル ネットワーク ポリシーに置き換えられます。

図 D-10　　例 7 で完成したポリシー



委任管理者の作成

次に、委任管理者を追加する必要があります。それには、管理可能なアクセス ポリシーを割り当てる委任管理者の、Web ユーザ ロールを作成する必要があります。

ユーザ ロールを定義するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [User Roles] を選択します。

ステップ 2　[Add Web User Role] をクリックします。

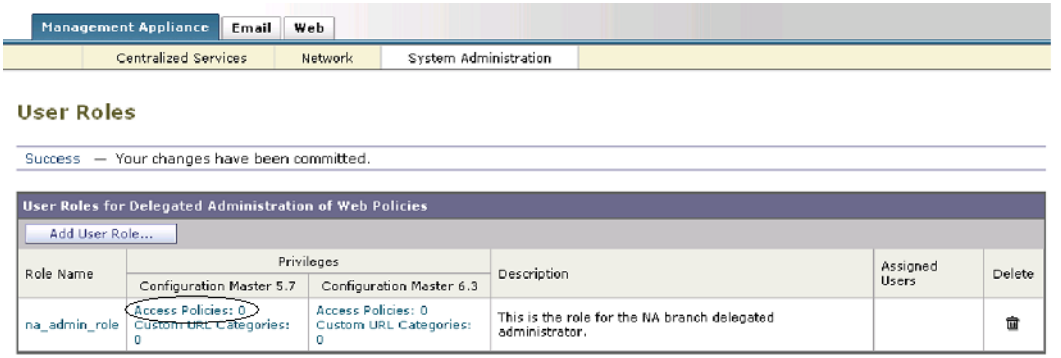
これにより、NA 拠点のユーザ ロールが追加されます。

ステップ 3　[Edit Web User Roles] ページの [Name] テキスト フィールドに **na_admin_role** と入力します。

ステップ 4　[Submit] をクリックします。

[User Roles] ページが表示されます。

ステップ 5　[Configuration Master 5.7] の下の [na_admin_role] 行で、[Access policies] をクリックします。



[Edit Access Policy Privileges: na_admin_role] ページが表示されます。

ステップ 6　[NA Access Policy] の横にあるチェックボックスをオンにして、NA 委任管理者用のユーザ ロールへの NA アクセス ポリシーを選択します。

ここでは、ソーシャル ネットワークのカスタム URL は、NA 拠点のユーザ ロールに追加されません。これは共有 URL カテゴリです。1 つのサイトでこれを変更すると、すべてのサイトに反映されます。このカテゴリは、メイン管理者の管理に任せることにします。これで、NA 拠点のユーザ ロール設定が完了しました。

委任ユーザのユーザ ロールが設定されたため、NA 拠点の委任管理者を作成できるようになりました。

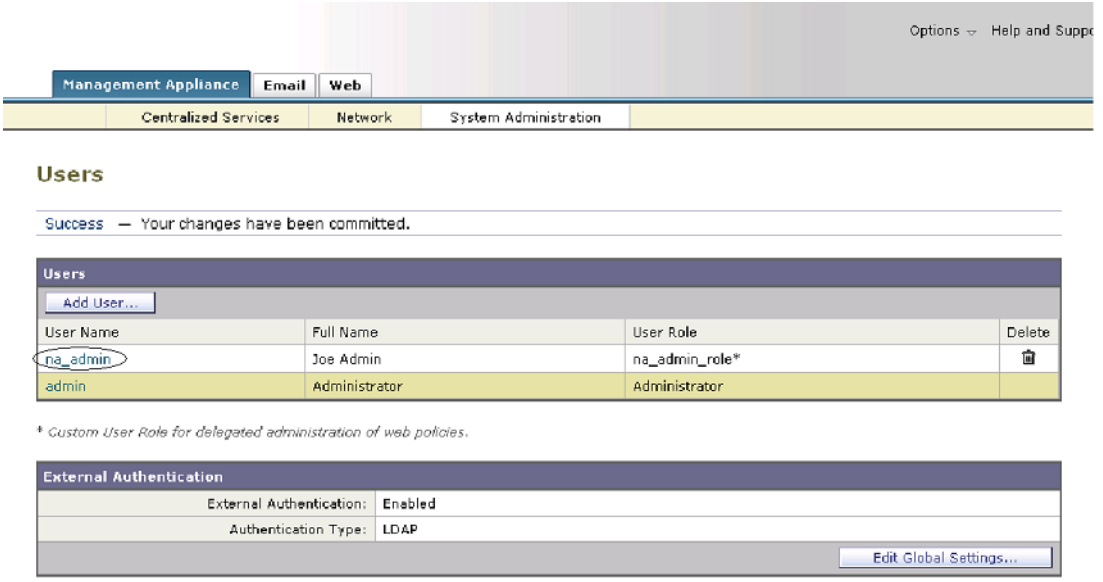
ステップ 7　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

ステップ 8　[Add User] をクリックします。

ステップ 9　[Custom Roles] オプション ボタンをクリックし、[Custom Roles] の下にあるウィンドウで [na_admin_role] を選択します。

ステップ 10　[Submit] をクリックします。

これで NA 委任管理者のロールが付与されます。



HQ 委任管理者のロールを持つユーザ ロールを新たに作成する必要があります。

ステップ 11　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

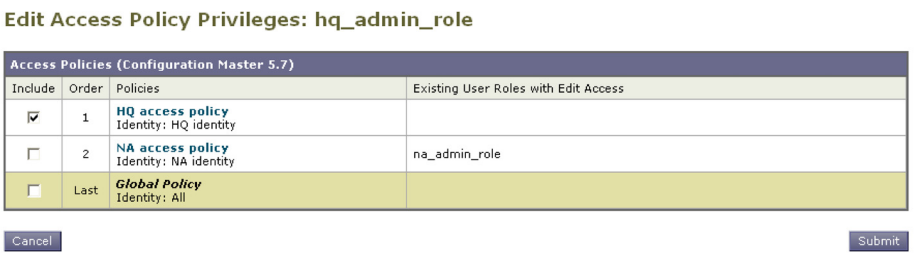
ステップ 12　[Add Users] をクリックします。

ステップ 13　[Edit User Roles] ページの [Name] テキスト フィールドに **hq_admin_role** と入力します。

ステップ 14　[Submit] をクリックします。

ステップ 15　[User Roles] ページにある [Configuration Master 5.7] の下の [hq_admin_role] 行で、[Access policies] をクリックします。

ステップ 16　[Edit Access Policies] ページで、[Include] チェックボックスをオンにして、HQ 委任管理者が HQ アクセス ポリシーを管理できるようにします。



ステップ 17　[Submit] をクリックします。

ステップ 18　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

ステップ 19　[Add User] をクリックします。

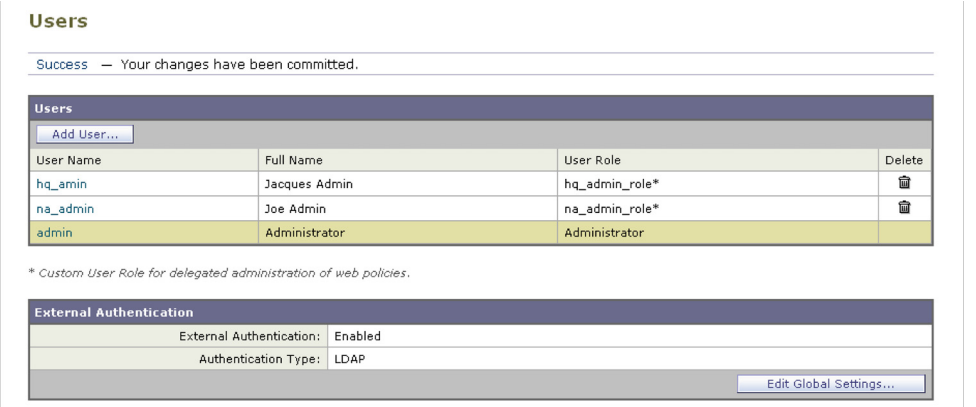
ステップ 20　[Custom Roles] オプション ボタンをクリックし、[Custom Roles] の下にあるウィンドウで [hq_admin_role] を選択します。

これで、HQ 管理者ロールが HQ 管理者に割り当てられます。

ステップ 21　[Submit] をクリックします。

図 D-11 に、割り当てられた委任管理者が表示された Users テーブルを示します。

図 D-11　　割り当てられた委任管理者



すべて完了しました。

これで、3 つの各ロケーションに、ユーザを識別する ID が作成されました。

この後、ロケーションに適切なアクセス ポリシーを作成し、ロケーションの ID を、ロケーションのカスタマイズされたアクセス ポリシーに追加しました。

さらに、AsyncOS 5.7 にはないカテゴリを追加するため、URL カテゴリを作成しました。

最後に、ローカルなアクセス ポリシーを維持するための委任管理者を作成しました。

関連項目

表 D-7 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-7　アクセス ポリシーのカスタマイズの関連項目

機能名	機能情報
[User] ページ	「[Users] ページ」（P.5-16）
[User Details] ページ	「[User Details] ページ」（P.5-20）
[Custom URL Categories] ページ	「カスタム URL カテゴリ」（P.5-33）