Domain Gateway オプションの環境構築における考慮点

1.はじめに

IceWall SSO Domain Gateway オプション（以下DGO）を使用して統合Windows認証環境を構築する際は、いくつか考慮すべき点があります。

本レポートでは、環境構築方法や設定方法の例を交えて以下の説明をいたします。

- DGO環境構築手順の例
- クライアントがWindows 7の場合の考慮点
- Microsoft Active Directory（以下MSAD）ドメインサーバーがWindows Server 2008 R2以降の場合の考慮点
- 統合Windows認証できない場合の確認点

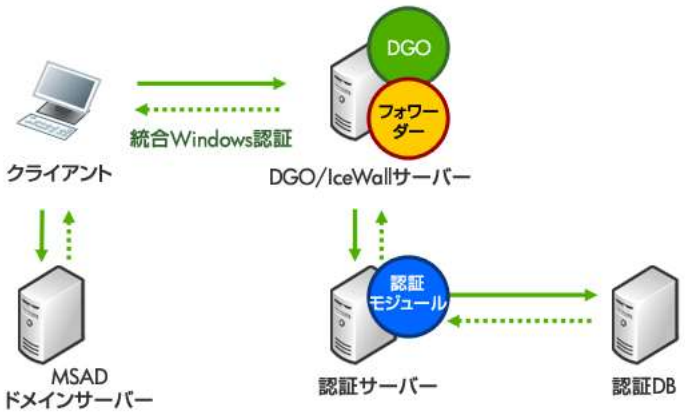
2.DGO環境構築手順の例

DGOで統合Windows認証を行う環境の構築手順の一例を紹介いたします。

以下で紹介する手順はDGOで統合Windows認証を行う環境を作成する手順の一例であって、こちらで説明する構築方法以外でも環境は構築できます。

2.1 システム構成図

例として記載するシステム構成は次の図のとおりです。



・IceWallサーバー
IceWall SSO バージョン情報：10.0
ホスト名：dgo.icewall.local

・MSADドメインサーバー
ホスト名：ad01.icewall.local
Kerberosチケットの解析で使用するユーザー名：dgouser01

・認証サーバー
IceWall SSO バージョン情報：10.0

・認証DB
データベース：Oracle Database 11g Release 2 Enterprise Edition
※DGOが参照するMSADサーバーに対して、認証モジュール（certd）の認証DBとして接続することも可能です。

2.2 MSADドメインサーバー上での手順

1.「DNSサーバー」の役割をインストールする。

2.「Active Directoryドメイン サービス」の役割をインストールする。

3. Kerberosチケットの解析で使用するユーザー「dgouser01」を作成する。

4. コマンドプロンプトを立ち上げ ktpassコマンドを実行する。

```
C:¥>ktpass -crypto [Kerberosチケットの暗号化方式] -princ [プリンシパル名(HTTP/FQDN@REALMS)] -mapuser [Kerberosチケットの解析で使用するユーザー名] -pass [パスワード] -ptype [プリンシパルの種類] -out [出力ファイル名]
```

※cryptoオプションに「RC4-HMAC-NT」を指定した場合は Kerberosチケットの暗号化方式に RC4が使用され、「DES-CBC-CRC」又は「DES-CBC-MD5」を指定した場合は DESが使用されます。特別な制限が無い場合は、RC4で設定されることをお勧めします。
※FQDNはホスト名が大文字の場合でも、小文字で指定する必要があります。
※REALMSは大文字で記述する必要があります。

コマンド実行例：

```
C:¥>ktpass -crypto RC4-HMAC-NT -princ
HTTP/dgo.icewall.local@ICEWALL.LOCAL -mapuser dgouser01 -pass
password -ptype KRB5_NT_PRINCIPAL -out C:¥dgoserver.keytab
Targeting domain controller: ad01.icewall.local
Using legacy password setting method
Successfully mapped HTTP/dgo.icewall.local to dgouser01.
Key created.
Output keytab to C:¥dgoserver.keytab:
Keytab version: 0x502
keysize 85 HTTP/dgo.icewall.local@ICEWALL.LOCAL ptype 1
```

```
(KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x8846f7eaee8fb117ad06bdd830b7586c)
```

5. ユーザーアカウントに関連付けされているSPNを確認する為にsetspnコマンドを実行する。

```
C:¥>setspn -L [ユーザー名]
```

コマンド実行例：

```
C:¥>setspn -L dgouser01
次の項目に登録されている CN=dgouser01,OU=icewall,DC=icewall,DC=local:
HTTP/dgo.icewall.local
```

6. MSADドメインサーバーで作成した「C:¥dgoserver.keytab」ファイルをIceWallサーバーに転送する。

2.3 IceWall サーバー上での手順

1. 作成したkeytab情報を追加する。

コマンド実行例：

```
# cp -p /etc/krb5.keytab /etc/krb5.keytab.backup
# ktutil
ktutil: read_kt dgoserver.keytab
ktutil: list
slot KVNO Principal
----------------------------------------------------------------------------------------------------
1 4 HTTP/dgo.icewall.local@ICEWALL.LOCAL
ktutil: write_kt /etc/krb5.keytab
ktutil: quit
```

2. keytabファイルのパーミッションを変更する。

コマンド実行例：

```
# chown apache:apache /etc/krb5.keytab
# ls -ltr /etc/krb5.keytab
-rw------- 1 apache apache 70 9月  7 06:50 /etc/krb5.keytab
```

3.「/etc/krb5.conf」ファイルを変更する。
設定ファイル内に「includedir /etc/krb5.conf.d/」の設定がある場合は、
ディレクトリ「/etc/krb5.conf.d/」が存在することを確認します。
ディレクトリが存在しない場合は、該当行をコメントアウトします。

設定例：

```
# includedir /etc/krb5.conf.d/
```

krb5-libsのバージョンが1.9(RHEL 6.1～RHEL6.3)の場合は、追加で以下の設定が必要です。
設定例：

```
[libdefaults]
default_realm = ICEWALL.LOCAL
```

4.「/etc/hosts」ファイルを変更する。

設定例：

```
127.0.0.1 localhost.localdomain localhost
191.168.0.XX dgo.icewall.local dgo
192.168.0.YY ad01.icewall.local ad01
```

※名前解決の候補を複数記述する場合は、FQDNを先に記述する必要があります。

5. DGOの導入ガイドを参照の上、インストールおよび設定を行う。

「dgfw.conf」設定例：

```
SERVICE_NAME=HTTP@dgo.icewall.local
```

2.4 クライアント端末上での手順

1. IceWallサーバー、およびMSADドメインサーバーの名前解決ができるようにDNS設定を行う。

2. クライアント端末をMSADドメインサーバーにドメイン参加させる。

3. Microsoft Internet Explorerを起動し、以下の順序で「インターネットオプション」を表示する。
[ツール(T)] – [インターネット オプション(O)]

4. 以下の順序で「ローカル イントラネット」の設定画面を表示する。
[セキュリティ タブをクリック] – [ローカル イントラネットを選択] – [サイトをクリック] – [詳細設定をクリック]

5. ローカルイントラネットにDGOサーバーを追加する。

設定例：

```
http://dgo.icewall.local
```

6. 以下の順序で「セキュリティ設定」の設定画面を表示する。
[セキュリティタブをクリック] – [ローカルイントラネットをクリック] – [レベルのカスタマイズをクリック]

7. 以下の順序でユーザー認証の設定を行う。
[ユーザー認証] – [ログオン] – [イントラネット ゾーンでのみ自動的にログオンする]

8. IceWallログインページの「統合Windows認証」からログインを行う。

※アドレス欄に指定するURLはIPアドレス形式での指定ではなく、ホスト名で指定する必要があります。

URL例：

```
http://dgo.icewall.local/fw/dfw/LOCALHOST/index.html
```

3.クライアントが Windows 7の場合の考慮点

DGOで統合Windows認証が既に行える環境に、新たに Windows 7のクライアントを追加する場合はサーバー側の設定確認が必要です。
Kerberos暗号化方式にDESを使用している場合は、Windows 7のセキュリティポリシーのデフォルト設定により統合Windows認証が許可されません。
Kerberos暗号化方式にRC4を使用している場合は、セキュリティポリシーの設定は必要ありません。

3.1 MSADドメインサーバーがWindows Server 2003 R2の場合、Kerberos暗号化方式にDESが使用されているかを確認する手順の一例

1. MSADドメインサーバー上で、Kerberosチケットの解析で使用するユーザーのプロパティーを表示します。

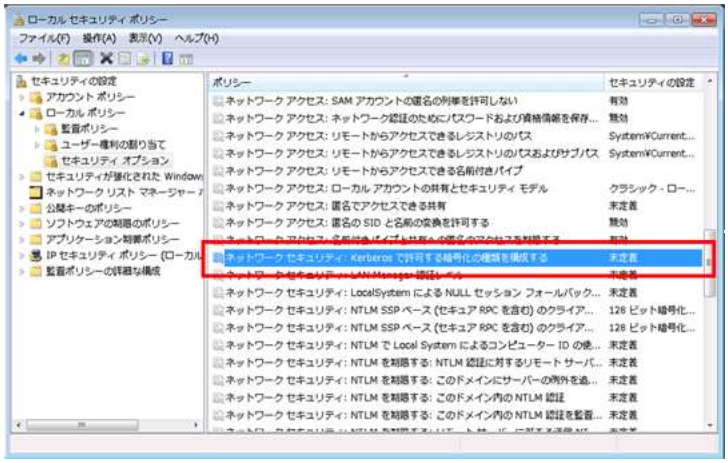
2.「アカウント」タブの「アカウントオプション」の項目を確認します。
「このアカウントにKerberos DES暗号化を使う」にチェックが入っている場合は、Kerberos暗号化方式にDESが使用されています。

3.2 Kerberos暗号化方式にDESを使用している場合の、Windows 7上でのセキュリティポリシー設定手順の一例

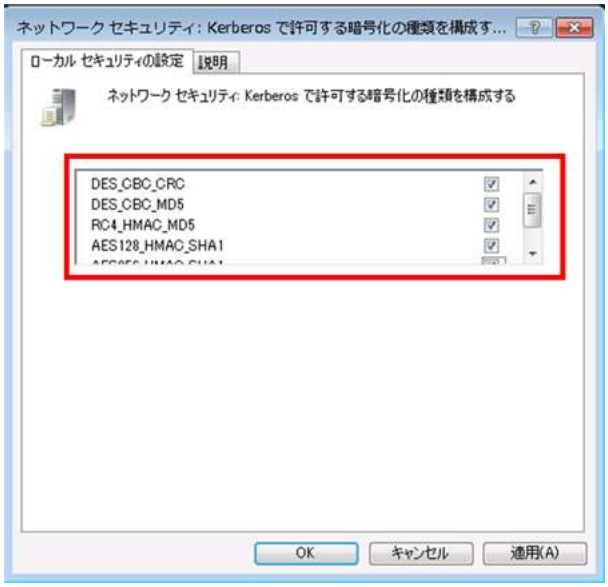
1. 管理者権限のアカウントでログインし、以下の順序でローカルセキュリティポリシーを起動する。
[コントロールパネル] – [管理ツール] – [ローカルセキュリティポリシー]

2. ローカルセキュリティポリシーの画面で、以下の項目を選択する。
[ローカルポリシー] – [セキュリティオプション]

3. 右側に表示されるポリシーから「ネットワークセキュリティ:kerberosで許可する暗号化の種類を構成する」をダブルクリックする。



4. 以下の項目にチェックを入れ、OKボタンをクリックする。
「DES_CBC_CRC」、「DES_CBC_MD5」、「RC4_HMAC_MD5」、「AES128_HMAC_SHA1」、
「AES256_HMAC_SHA1」
※使われない暗号化の種類はチェックを外しておくことをお勧めします。



5. セキュリティポリシーを有効にするため、マシンの再起動を行う。

4. MSADドメインサーバーが Windows Server 2008 R2以降の場合の考慮点

Kerberosチケットの暗号化方式にDESを使用している場合は、Windows Server 2008 R2のセキュリティポリシーのデフォルト設定により統合Windows認証が許可されません。

Kerberosチケットの暗号化方式にRC4を使用している場合はセキュリティポリシーの設定は必要ありません。

Kerberosチケットの暗号化方式がRC4の環境を新規に構築する場合の構築手順は、「2.DGO環境構築手順の例」を参照してください。

Kerberosチケットの暗号化方式がDESで既に構築されている場合は、MSADドメインサーバー側のセキュリティポリシーの設定が必要です。

設定手順については、「3.2 Kerberos 暗号化方式にDESを使用している場合の、Windows 7上でのセキュリティポリシー設定手順の一例」を参照してください。

5. 統合Windows認証できない場合の確認点

統合Windows認証でログインできない場合のよくある問題として以下が考えられます。

- クライアントからIceWallサーバーにKerberosチケットが送られていない
- REALMを大文字で統一していない
- MSADドメインサーバー、IceWallサーバー、クライアントの時刻が大きくずれている

6.まとめ

Windows Server 2008 R2およびWindows 7の場合は、セキュリティポリシーのデフォルト設定によりKerberosチケットの暗号化方式にDESが許可されません。
Kerberosチケットの暗号化方式にRC4を使用している場合はセキュリティポリシーの設定は必要ありません。
DGOの環境をこれから構築される場合は、セキュリティの観点からもメリットがあるRC4での環境構築をご検討ください。

ご参考URL
≫Windows 7およびWindows Server 2008 R2におけるKerberos認証の変更点

関連技術レポート
技術レポート：Active Directory環境でのIceWallへのアクセス（信頼関係を結んでいる複数ドメイン編）
技術レポート：Active Directory環境でのIceWallへのアクセス（信頼関係を結んでいない複数ドメイン編）

2010.11.30 新規掲載
2018.5.15 見出し2を加筆修正
2019.10.2 見出し2を加筆修正

執筆者
日本ヒューレット・パッカード テクノロジーコンサルティング統括本部 テクニカルコンサルタント 神原 健太