



【連携機器】Citrix NetScalar 【Case】証明書と ID・Password によるハイブリッド認証 Rev1.0

株式会社ソリトンシステムズ

はじめに

本書について

本書は、NetAttest EPS と Citrix 社製 VPN ゲートウェイ NetScalar との証明書+ID・ Password 認証連携について記載した設定例です。 各機器の管理 IP アドレス設定など、基本設定は既に完了しているものとします。設定は管 理者アカウントでログインし、設定可能な状態になっていることを前提に記述します。

表記方法

表記方法	説明
ſJ	参照するドキュメントを示します。
٢J	参照する章、節、ボタンやメニュー名、強調する単語を示します。
[+-]	キーボード上のキーを表します。
[+-1]+[+	「七-1」を押したがら「七-2」を押すことを表します
-2]	

表記方法(コマンドライン)

表記方法	説明
%, \$, >	一般ユーザーのプロンプトを表します。
#	特権ユーザーのプロンプトを表します。
[filename]	[] は省略可能な項目を示します。この例では、filename は省
[mename]	略してもよいことを示しています。



アイコンについて

アイコン	説明
•	利用の参考となる補足的な情報をまとめています。
	注意事項を説明しています。場合によっては、データの消失、
<u> </u>	機器の破損の可能性があります。

画面表示例について

このマニュアルで使用している画面(画面キャプチャ)やコマンド実行結果は、実機での表示と若干の違いがある場合があります。

ご注意

本書は、当社での検証に基づき、NetAttest EPS 及び NetScalar の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

NetAttest®は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。 本文中に ™、®、©は明記していません。

目次

1. 構成
1-1 構成図6
1-2 環境7
1-2-1 機器7
1-2-2 認証方式7
1-2-3 ネットワーク設定7
2. NetAttest EPSの設定8
2-1 システム初期設定ウィザードの実行8
2-2 サービス初期設定ウィザードの実行9
2-3 認証ユーザーの追加登録10
2-4 クライアント証明書の発行11
3. NetScalar の設定12
3-1 各インターフェイスの設定12
3-2 機能の有効化14
3-3 サーバー証明書、CA 証明書のダウンロードとインポート手順 15
3-3-1 CSR の作成(NetScalar)16
3-3-2 サーバー証明書のダウンロード (NetAttest EPS)
3-3-3 CA 証明書のダウンロード (NetAttest EPS) 21
3-3-4 サーバー証明書のインポート (NetScalar)
3-3-5 CA 証明書のインポート (NetScalar) 24
3-4 OCSP の設定 25
3-4-1 OCSP 署名証明書の発行(NetAttest EPS)
3-4-2 OCSP に関する設定(NetScalar)
3-5 RADIUS ポリシーの設定 30
3-6 セッションポリシーの設定 32
3-7 Virtual Serverの設定34
4. VPN クライアントの設定38
4-1 PC へのデジタル証明書のインストール
4-2 NetScalar Gateway Plug-in のインストール



1. 構成

1-1構成図



1-2環境

1-2-1機器

製品名	メーカー	役割	バージョン
NetAttest EPS-ST04	Soliton Systems	認証サーバー (RADIUS サーバー、CA)	Ver. 4.6.8
NetScalar MPX-5550	Citrix	RADIUS クライアント (SSL VPN 機器)	Ver. 10.5
GW-MF54G2	PCi	無線 AP (インターネット側用)	-
Let's note CF-SX2	Panasonic	Client PC	Windows 7 SP1

1-2-2認証方式

デジタル証明書認証+ID・Password 認証

1-2-3ネットワーク設定

	EPS-ST04	NetScalar MPX-5550	Client PC	無線 AP
IPアドレス	192.168.1.2/24 (LAN1) 192.168.2.1/24 (LAN2)	192.168.3.11/24(external) 192.168.3.10/24(external) 192.168.1.11/24(manage) 192.168.1.10/24(internal)	DHCP (無線 AP から)	192.168.1.100/24
RADIUS port (Authentication)	UDP 1812		_	_
RADIUS Secret (Key)	secret		-	-

2. NetAttest EPS の設定

2-1システム初期設定ウィザードの実行

http://192.168.2.1:2181(LAN2 デフォルト)にアクセスしシステム初期設定ウィザードを使用し

初期設定ウィザードー設定項目の確認

- て、以下の項目を設定します。
- タイムゾーンと日付・時刻の設定
- ホスト名の設定
- サービスインターフェイスの設定
- 管理インターフェイスの設定
- ドメインネームサーバーの設定

設定内容を確認って下さい。 この設定を保存・反映するには「再起動」ボタンを・	リックレて下さい。
キットワーク時刻	
N1P9-J	
NIP9-)	
Net Allest EPS	146 無効
ቱ .አዞ 8	
サービスインターフェイス	
Te IIIndato II-II IP21	
2.2.2.4.10月前全	
 * 2.世ス語見放え CA51センス 	
4월 <u>227人里#1-7</u> 4	
en an	
עכ	
1985(t)2	
最大ユーザ	
Elegenen e 2004 2010, Solten Teynenin K.K., All nem mennet Elegenen e 2004 2010, Solten Teynenin K.K., All nem mennet	
外部9~六一篇	18 有効
RADIUS70	
WindowsFメイン認識	an 無功
ઝામ	
MACZEUZI	ar 無効
#-+1	神 無効
	戻る 再起動

2-2サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

本手順書では値を記載しているもの以外はすべてデフォルト設定で行いました。

- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定(全般)
- RADIUS サーバーの基本設定(証明書検証)
- NAS/RADIUS クライアント設定

CA種別選択			
CA種別選択	<i>μ</i> -+ca ▼		
CA秘密鍵			
◎ 内部で新しい鍵を生成する			
公開鍵方式	RSA -		
鍵長	2048 👻		
◎ 外部HSMデバイスの鍵を使用す			
要求の署名			
要求署名アルゴリズム	SHA1 -		
CA情報			
CA名(必須)	TestCA		
国名	指定しない		
都道府県名			
市区町村名		項目	値
会社名(組織名)			
部署名		CA 種別選択	ルート CA
E-mailアドレス		公開鍵方式	DCV
CA署名設定		ム田町近り工	RSA
署名アルゴリズム	SHA1 -	。 鎌長	2048
有効日数	3650		2070
	展る 次へ	CA 名	TestCA



項目	値
NAS/RADIUS	NetScalar
クライアント名	
IP アドレス	192.168.1.10
(Authenticator)	
シークレット	secret

- 9 -



2-3認証ユーザーの追加登録

Copyright © 2004-2011, Soliton Systems K.K., All rights res

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

「ユーザー」→「ユーザー一覧」から、「追加」ボタンでユーザー登録を行います。



2-4クライアント証明書の発行

NetAttest EPS の管理画面より、クライアント証明書の発行を行います。

「ユーザー」→「ユーザー一覧」から、該当するユーザーのクライアント証明書を発行します。(ク ライアント証明書は、user01_02.p12 という名前で保存)

Not 'Attert EBC			
NGI MIGSI EFS			(1トッブページ 回 設定保存 10 ログオフ
■ naeps00.local	🚬 ユーザー一覧		
 システム設定 システム管理 	フーザー ● 一部 ● 完全 グルー	ォ ❤ 1000 ユーザーまで 検索	
■ 証明機関			追加
■ DHCPサーバー			ユーザー削除時の証明書失効オプション
■ RADIUSサーバー	<u>名前</u>	<u>ユーザーID</u>	新明書 タスク
- 7-+f-	test user	test	発行 変更 削除
コーザー一覧	user01	<u>user01</u>	発 変更 削除
			Y
		編集対象: user01	
		基本情報	
		姓	user01
		名	
		E-Mail	
		詳細情報	< >
		認証情報	
		ューザーm	user01
		有効期限・	
		● 日付 2013 V 年 2 V 月	28 × 日 23 × 時 59 × 分 59 × 秒まで
		証明書ファイルオブション	
百日	値	パスワード	
	믹	バスワード(確認)	
証明書有効期限	365	×バスワードが空間の場合には、ユーザー	ーのパスワードを使用します。
		☑ PKCS#12ファイルに証明機関の証明	書を含める
PKCS#12 ファイルに	証明機関の・・ チェック有		発行キャンセル
	ューザー証明書のダウンロ	-F	
	- エーリー証明書タリンロート	の卒順かでさました。対家をノアイルI 	



3. NetScalar の設定

3-1各インターフェイスの設定

NetScalar の各インターフェイスの設定を行います。

管理インターフェイスの IP アドレスはデフォルトで「192.168.100.1」ですので、ブラウザより 「http://192.168.100.1/」でアクセスします。

「User Name」「Password」はどちらも「nsroot」ですので、入力後「ログイン」をクリックします。

User Name Insrot To use https, click here Dogin		
CITDLY:	To use https, click here	User Name nsroot Password •••••• Login
Copyright(®) Citrix Systems, Inc. All rights reserved.	c	opyright(@) Citrix Systems, Inc. All rights reserved.

項目	値
User Name	nsroot
Password	nsroot

ログイン後、[Network]-[IPs]より[IPV4s]タブの「Add」をクリックし、各インターフェイスの設 定を行います。

各インターフェイスの「Type」は以下です。

NetScalar IP:管理用

Subnet IP:Internal 用

Virtual IP:external 用

Dashboard	Configuration	Reporting
+ Back		
Configure IP A	ddress	
IP Address		1
192 . 168 .	1 . 10	
Netmask		
255 . 255 .	255 0	
Туре		
Subnet IP		
Mode		
Active		
Virtual Router ID		
	⊻ ?	
ICMP Response*		
NONE	\checkmark	
ARP Response*		
NONE		

項目	値
NetScalar IP	192.168.1.11
Subnet IP	192.168.1.10
Subnet IP	192.168.3.11
Virtual IP	192.168.3.10

NetScaler > System	> Network > If	Ps > IPV4s					¢ 😗 🖬
IPV4s IPV6s							
Add Edit	Delete	Statistics Action	•				Search 🔻
IP Address	State	Туре	Mode	ARP	ICMP	Virtual Server	Traffic Domain
▶ 192.168.1.11	Enabled	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0
▶ 192.168.1.10	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0
▶ 192.168.3.10	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED	0
▶ 192.168.3.11	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0

3-2機能の有効化

機能を有効にします。

[System]-[Settings]より「Configure Basic Features」をクリックします。

「SSL Offloading」、「NetScalar Gateway」をチェックし、「OK」をクリックします。

Dashboard	Configuration	Reporting			Documentation	Downloads	ł
- System		NetScaler > System	> Settings			0	?
Licenses							
Settings		Modes and Featu	ures	Settings			
Diagnostics		Configure modes		Change Global System	Settings		
High Availabili	ity	Configure Basic Feature	5	Change NSVLAN settir	igs		
NTP Servers		- conguerra anceurra		Change TCP paramete	rs		
Reports				Change Diameter para	meters		
Profiles				Change Encryption par	rameters		
+ User Administ	ration			Change Timeout Value	5		
+ Authentication	1			Change RSS Key Type			
+ Auditing							
+ Auditing + SNMP	Ĩ						
+ Auditing + SNMP	ler (5550)	¥			lnfo N\$10.5 51.10.nc	✓ Logout	ci
+ Auditing + SNMP + Auditing + SNMP + Auditing + SNMP	ler (5550)	Reporting			info NS10.5 51.10.nc Documentation	 Logout Downloads 	ci
+ Auditing + SNMP SINCTSCA Dashboard	ler (5550)	Reporting			info NS10.5 51.10.nc Documentation	▼ Logout Downloads	ci
+ Auditing + SNMP A SPINN NetSca Dashboard ← Back Configure Bas	ler (5550) Configuration	Reporting			iofo N510.5 51.10.nc Documentation	Logout Downloads	ci
+ Auditing + SNMP A Softward NetSca Dashboard ← Back Configure Bass ✓ SSL Offloadir	ler (5550) Configuration sic Features	Reporting	n		¹⁰¹⁰ N510.5 51.10.nc Documentation	Logout Downloads	ci
+ Auditing + SNMP A AUGUAN NetSca Dashboard + Back Configure Bas SL Offloadir Load Balanci	Configuration	Reporting	on g		into NS10.5 51.10.nc Documentation	Logout Downloads	di
+ Auditing + SNMP August August NetSca Dashboard ← Back Configure Bass ✓ SSL Offloadir Load Balanci Content Fille Permit	ler (5550) Configuration cic Features	Reporting	on g ng		Info NS10.5 S1.10.nc Documentation	Logout Downloads	ci
+ Auditing + SNMP SNMP Auditing * SNMP Auditing NetSca Dashboard Configure Bask Configure Bask SSL Offloadit Load Balanci Content Filte Rewrite Authenticatic	ler (5550) Configuration cic Features	Reporting	on g ng ay		Info NS10.5 51.10.nc Documentation	Logout Downloads	ch
+ Auditing + SNMP SNMP Austrian NotSca Dashboard ← Back Configure Base SSL Offloadin Load Balanci Content Filte Rewrite Authentication	Configuration cic Features	Reporting	on g ng ay azall		Info NS10.5 51.10.nc Documentation	Logout Downloads	cit

3-3サーバー証明書、CA 証明書のダウンロードとインポート手順

以下の手順でサーバー証明書と CA 証明書を NetScalar にインポートします。

- CSR の作成(NetScalar)
- サーバー証明書ダウンロード(NetAttest EPS)
- CA 証明書のダウンロード(NetAttest EPS)
- サーバー証明書のインポート(NetScalar)
- CA 証明書のインポート(NetScalar)

3-3-1CSR の作成(NetScalar)

Key の作成を行います。

[Traffick Management]-[SSL]より「Create RSA Key」をクリックします。

「Key Filename」、「Key Size」を入力し、「OK」をクリックします。

Dashboard	Configuration	Reporting		Documentation	Downloads	\$
+ System		NetScaler > Traffic Managem	ent > SSL		¢ (3)	
+ AppExpert						
- Traffic Management		Getting Started		SSL Certificates		
+ Load Balancing		Server Certificate Wizard		Create CSR (Certificate Signing Request)		
+ Content Switching	Ū.	Intermediate-CA Certificate Wiz	ard	Create and Install a Server Test Certificate		
+ Cache Redirection		Root-CA Certificate Wizard				
+ DNS		cite management				
+ GSLB	()	SEL Keye		Tools		
- SSL		Create RSA Key		Create Diffie-Hellman (DH) key		
Certificates	_	Create I SA Key		Import PKCS#12 Export PKCS#12		
Cipner Group:	s			Manage Certificates / Keys / CSRs		
Policies				Start SSL certificate, key file synchronization for HA Start SSL certificate, key file synchronization for Clu	a uster	
Policy Labels				OpenSSL interface		
OCSP Respon	der					
Imports		SSL Policy Manager		Change advanced SSL settings		
Dashboard	Configuration	Reporting		Documentation	Downloads	\$
+ Back						0
Create RSA Key						
Key Filename*						
		Browse 👻				
Key Size(bits)*						
Public Exponent Value	*					
3	\checkmark					
Key Format*						
PEM	×					
PEM Encoding Algorith	nm					
	•					
PEM Passphrase						
Carfan DEM Davahar						
Commit PEW Passphra	150					
OK Close						
TRE	15	5				

項目	値
Key Filename	Soliton.key
Key Size	2048



CSR の作成を行います。

[Traffick Management]-[SSL]より「Create CSR」をクリックします。

「Request File Name」を入力し、「Key Filename」にて、先ほど作成した Key を選択します。

「Distinguished Name Fields」にてサブジェクトを入力します。



項目	値
Request File Name	Soliton.csr
Key Filename	Soliton.key



Key Format			
● PEM ○ DER			
DEM Dassonbrase (For Encrypted Key)			
Distinguished Name Fields			
Country*			
UNITED STATES			
State or Province*			
Organization Name*			
City			
Email Address			
Organization Unit			
Common Name			
Challenge Deserved			
伯日	伯		

項目	値
Country	Japan
Organization Name	Soliton
Common Name	192.168.3.10

CSR のダウンロードを行います。

[Traffick Management]-[SSL]より「Manage Certofocates/Keys/CRLs」をクリックします。

作成した CRL を選択し、「Download」をクリックします。

Dashboard	Configuration	Reporting	Documentation Downloads 🄅
+ System		NetScaler > Traffic Management > SSL	
+ AppExpert - Traffic Management + Load Balancing + Content Switchi + Cache Redirection + DNS	nt 1 ing 1 ion 1	Getting Started Server Certificate Wizard Client Certificate Wizard Intermediate-CA Certificate Wizard Root-CA Certificate Wizard CRL Management	SSL Certificates Create CSR (Certificate Signing Request) Create Certificate Create and Install a Server Test Certificate
+ GSLB - SSL Certificates Cipher Grou CRL Policies Policy Labe	ups	SSL Keys Create RSA Key Create DSA Key	Tools Create Diffie-Hellman (DH) key Import PKCS#12 Manage Certificates / Keys / CSRs Control Confiction (Confiction of the Astronomy of the A
OCSP Resp Imports	onder	Policy Manager SSL Policy Manager	Settings Change advanced S. L. settings
Manage Certifica	tes Directory: /nsconfiq/ss	м/	•
Download Up	load View	Delete Create Directory	
	ы п Е	ile reprudry 04 2014 11:57:10	restruary 03 2014 11:22:19
toa-mpx_test-p	em.cer F	le rebruary 04 2014 15:50:14	March 21 2014 12:36:16
nacacert-pem.c	er F	ile February 06 2014 10:52:27	March 21 2014 12:36:16
itoa-mpx_public	csr F	ile February 05 2014 11:30:35	February 05 2014 11:31:09
📄 toa-mpx_public	-pem.cer F	ile February 05 2014 11:37:13	March 21 2014 12:36:16
soliton.key	F	ile August 29 2014 14:23:53	August 29 2014 14:34:00
isoliton.csr		le August 29 2014 14:24:48	August 29 2014 14:24:59
a.cer	F	ie August 29 2014 14:32:38	August 29 2014 14:34:37
inacacri.crl	F	ile August 29 2014 14:32:43	August 29 2014 14:32:43
server.cer	F	ile August 29 2014 14:32:47	August 29 2014 14:34:00
Close			



3-3-2サーバー証明書のダウンロード (NetAttest EPS)

NetScalar で生成した CSR をもとに NetAttest EPS で NetScalar 用サーバー証明書を発行します。 NetAttest EPS の管理者向け証明書サービスページ(http://192.168.2.1/certsrva/)にアクセスし、 下記の手順で CSR をインポートします。

Net Attest EPS			
= naeps00.local	証明書要求-プロファイルの選択		
■ CA情報 ■ ダウンロード	このPCでは、以下の証明書要求を作成できます。		
■ 証明書要求 - 新明書変詞	<u>WEBサーバー証明書</u>		
	•		
要求の作成			
WEBサーバー証明書			
<u>PKCS#10ファイルによる証明書要求を閉じる</u>			
	参照		

次に、CA 管理ページ(http://192.168.2.1:2181/caadmin/)にアクセスし、【保留】状態のサーバ ー証明書を承認します。

要求リスト						
大熊 保留のみ表示 ✓ 更新 詳細オブションの設定						
	状態	<u>受付日時</u>	送信元	<u> プロファイル</u>		
	保留	2012/02/29 22:07:19	CAadm: 192.168.2.212:Mozilla/4.0 (compatible; MSIE 8.0; Windows	WEBサーバー証明書		
拒否 削除 発行: 有効日数 デフォルト 発行						

理者向け証明書サービスページにアクセスします。「証明書の確認」を選択すると状態が【発行】に なっていますので、サーバー証明書(nausercert-pem.cer)をダウンロードします。

状態 申請日時 プロファイル 証明書目的 申請者 タスク 発行 2013/02/01 16:24:26 WEB サーバー証明書(unknown) CN=soliton.co.jp,O=Soliton System インストール ダウンロード 削除	■要求一覧	-						
発行 2013/02/01 16:24:26 WEB サーバー証明書(unknown) CN=soliton.co.jp,O=Soliton System インストール ダウンロード 削除	状態	<u>申請日時</u>	プロファイル	証明書目的	<u>申請者</u>		タスク	
		2013/02/01 16:24:26	WEBサーバー証明書	(unknown)	CN=soliton.co.jp,O=Soliton System	インストール	ダウンロード	削除



3-3-3CA 証明書のダウンロード (NetAttest EPS)

管理者向け証明書サービスページから、NetAttest EPS の CA 証明書をダウンロードします。CA 証明書は、PEM 形式(nacacert-pem.cer)を選択します。

NetAttest EPS							
■ naeps.local	ダウンロード						
 ダウンロード 証明音架次 	CA証明書	ダウンロード <u>PEM</u> DER					
□ 証明書確認	<u>CA証明書</u>	インストール					
	CRLダウン	ロード <u>PEM</u> <u>DER</u>	最終更新日時: 2013/01/29 10:40:42				

3-3-4サーバー証明書のインポート (NetScalar)

サーバー証明書のインポートを行います。

[Traffick Management]-[SSL]より「Manage Certofocates/Keys/CRLs」をクリックします。

を選択し、「Upload」をクリックします。

[3-3-2]でダウンロードしたサーバー証明書をアップロードします。また[3-3-3]でダウンロードした CA 証明書もアップロードします。

Dashboard	Configuration	Reporting	Documentation Downloads 🄅
+ System		NetScaler > Traffic Management > SSL	♦ 1 Ø H
+ AppExpert			
- Traffic Managemer	nt	Getting Started	SSL Certificates
+ Load Balancing		Server Certificate Wizard	Create CSR (Certificate Signing Request)
+ Content Switchi	na 🕕	Intermediate-CA Certificate Wizard	Create and Install a Server Test Certificate
+ Cache Redirection	on	Root-CA Certificate Wizard	
+ DNS		CRL Management	
+ GSLB	()	SSI Kevs	Tools
— SSL		Create RSA Key	Create Diffie-Hellman (DH) key
Certificates		Create DSA Key	Import PKCS#12
Cipher Grou	ups		Export PK65/11 Manage Certificates / Keys / CSRs
CRL			Charles the state of the state
Policies			Start SSL certificate, key file synchronization for Cluster
Policy Labe	ls		Opensise interface
OCSP Resp	onder	Policy Manager	Settings
Imports		SSL Policy Manager	Change advanced S.L settings
Current	Directory: /nsconfig/ss	a/	
Download Up	load View	Delete Create Directory	
		Teorem 04 2014 13:57:10	C-herrer (05 2014 11-22-10
mpx_csr	F	lle February 04 2014 13:50:14	February 05 2014 11:22:19
toa-mpx_test-p	em.cer F	ile February 04 2014 14:04:36	March 21 2014 12:36:16
nacacert-pem.c	er F	ile February 06 2014 10:52:27	March 21 2014 12:36:16
itoa-mpx_public	_csr F	ile February 05 2014 11:30:35	February 05 2014 11:31:09
📄 toa-mpx_public	-pem.cer F	ile February 05 2014 11:37:13	March 21 2014 12:36:16
📄 soliton.key	F	ile August 29 2014 14:23:53	August 29 2014 14:34:00
📄 soliton.csr	F	ile August 29 2014 14:24:48	August 29 2014 14:24:59
i ca.cer	F	ile August 29 2014 14:32:38	August 29 2014 14:34:37
inacacrl.crl	F	ile August 29 2014 14:32:43	August 29 2014 14:32:43
i server.cer	F	ile August 29 2014 14:32:47	August 29 2014 14:34:00
Close			

[SSL]-[Certificates]より「Install」をクリックし、NetAttest EPS からダウンロードしたサーバー 証明書と CA 証明書を NetScalar にインストールします。

まずは、サーバー証明書をインストールします。

「Certificate-Key Pair Name」を入力し、「Certificate File Name」に[3-3-4]でアップロードした サーバー証明書を選択し、「Key file Name」には[3-3-1]で作成した「RSA Key」を選択します。

Dashboard Configuration Reporting	Documentation	Downloads	\$
← Back			•
Install Certificate			
Certificate-Key Pair Name*			
Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance. Certificate File Name*			
Key File Name Browse			
ertificate Format ● PEM ○ DER ⑦			
Password			
Certificate Bundle Notify When Expires Notification Period			
30			

項目	值
Certificate-Key Pair Name	soliton-server-certificate
Certificate File Name	[3-3-4]でアップロードしたサーバー証明書を選択
Key File Name	[3-3-1]で作成した RSA Key を選択(Soliton.key)

3-3-5CA 証明書のインポート (NetScalar)

次に CA 証明書をインストールします。

同じく「Install Certificate]より、「Certificate-Key Pair Name」を入力し、「Certificate File Name」 に[3-3-4]でアップロードした CA 証明書を選択します。

※「Key File Name」の選択は必要ありません。

Dashboard Configuration Reporting	Documentation I	Downloads	۵
← Back			?
Install Certificate			
Certificate-Key Pair Name*			
Certificate File Name* Browse			
Key File Name Browse			
Certificate Format ● PEM ○ DER ⑦			
Password			
Certificate Bundle Notify When Expires Notification Period			
30			
項目	値		

Certificate-Key Pair Name	soliton-root-certificate
Certificate File Name	[3-3-4]でアップロードした CA 証明書を選択

Dashboard Con	figuration	Reporting	Documentation Down	loads 🔅
System		NetScaler > Traffic Management > SSL > SSL Certificates		≎ @ 🖬
r AppExpert				Search ▼
 Traffic Management 			Dura to Funita Cata	- Scaren
+ Load Balancing		ivane	Days to Expire State	B
+ Content Switching	•	Insisterver-ceruncate	5526 Valid	
+ Cache Redirection	•	soliton-server-certificate	364 Válic	
+ DNS		soliton-root-certificate	3648 Valio	
+ GSLB	(!)			
- SSL				
Certificates				
Cipher Groups				
CRL				
Policies				
Policy Labels				
OCSP Responder				
Imports				
Optimization				
+ Security				
► NetScaler Gateway				



3-40CSPの設定

NetScalar が OCSP を使用して、認証毎に NetAttest EPS に証明書の失効確認を行う設定をします。

3-4-10CSP 署名証明書の発行(NetAttest EPS)

NetAttest EPS 管理ページより、[証明機関]-[CA 設定]-[OCSP 署名証明書]の「証明書を更新する」 をクリックします。

※NetAttest EPS が OCSP レスポンダとして動作するには、拡張 CA ライセンスが必要です。



3-4-20CSP に関する設定(NetScalar)

NetScalar 側で OCSP に関する設定を行います。

[Traffick Management]-[SSL]-[OCSP Responder]より「Add」をクリックします。

「Name」と「URL」を入力します。

NetAttest EPSのOCSP ResponderのURLは「http://<EPSのIP(FQDN)>:8088/」です

Dashboard Configuration	Reporting	Documentation Do	wnloads 🄅
+ System	NetScaler > Traffic Management > SSL > OCSP Responder		¢ 0
+ AppExpert	Add Edit Delete		Search 💌
	Name URL Cache Batching Depth Response Verification		Nonce
+ Content Switching			
+ DNS			
+ GSLB (!)			
·· Certificates			
CRL			
Policies Policy Labels			
OCSP Responder			
+ Optimization			
+ Security			
+ NetScaler Gateway			
Show Unlicensed Features			
Integrate with Citrix Products			

Dashboard Configuration	Reporting	Documentation	Downloads	۵
+ Back				0
Configure OCSP Responder				
Name epsocsp URL* http://192.168.1.28088/ Cache Time-out 1 min Request Batching	utes			
Batching Depth*				
Batching Delay				
Response Verification				
Produced At Time Skew				
300 seco	onds			
Certificate	Z			
Request Time-out				
2000 milli	iseconds			

項目	値
Name	epsocsp
URL	http://192.168.1.2:8088/

続いて NetScalar にインストールした CA 証明書に OCSP 設定を紐付けます。

[Traffick Management]-[SSL]-[Certificates]よりインストールした CA 証明書

(soliton-root-certificate)を選択し、「Action」のプルダウンメニューより「OCSP Bindings」をクリックします。

「OCSP Bindings」の右上のペンアイコンをクリックし、その後「Bind」をクリックします。

Dashboard Configuration	Reporting		Documentation	Downloads 🔅
+ System	NetScaler > Traffic Management > SSL > SSI	Certificates		0
+ AppExpert	Install Undate Delete Action	•		Search ¥
- Traffic Management	News Select	Action	Dava ta Evalua	Search -
+ Load Balancing 🔋	h ps-server-certificate		5516	Valid
+ Content Switching	soliton-server-certificate		352	Valid
+ Cache Redirection	h soliton-root-certificate		3636	Valid
+ GSLB	OpenSSI CA		3571	Valid
- SSL			3621	Valid
Certificates	 ansRootCA 		36/8	Valid
Cipher Groups	P epsiloner		363	Valid
CRL	k entSenjer2		363	Valid
Policies Policy Labels	p epsServer2		3648	Valid
OCSP Responder	Pepsitorick2		3640	Valid
+ Security + NetScaler Gateway Show Unlicensed Features netgrate with Citrix Products XenMobile				
Dashboard Configuration	Reporting		Documentation	Downloads 🐇
← Back				
Certificate-Key Pair Name soliton-root-certificate OCSP Bindings				
	Priority OCSP Responder Name			
No items	, , , , , , , , , , , , , , , , , , , ,			
Done				

+ Back	
Certificate-Key Pair Name	
soliton-root-certificate	
Bind Unbind Regenerate Priorities Edit	Sear

先ほど作成した「OCSP Responder」設定をチェックし、「Insert」をクリックします。その後「Done」 をクリックします。

Dashboard Configuration Reporting				Documentation	Downloads	\$	
	OCSP Responder						
	OCSP Responder						×
Certificate-Key Pair Name	Add Edit	Delete					Search 👻
soliton-root-certificate	Name	URL	Cache	Batching Depth Respon	nse Verification		Nonce
Bind Unbind Regenerate Priorities E	✓	http://192.168.1.2:8088/	Disabled	1 Basic			Enabled
Priority OCSP Responder Name	Insert Close						0
No items							
C Core							
Dashboard Configuration Report				Docum	entation	Downloads	æ
+ Back							T
Certificate-Key Pair Name soliton-root-certificate							
OCSP Bindings							/
	Priority OCSP R	Responder Name					
	1 epsocs	p					
Done							

3-5RADIUS ポリシーの設定

NetScalar で RADIUS ポリシーの設定を行います。

[NetScalar Gateway]-[Policies]-[Authentication]-[RADIUS]より「Servers」タブの「Add」を クリックします。

「Name」、「IP Address」、「Port」、「Secret Key」を入力し、「Create」をクリックします。

← Back	•
Create Authentication RADIUS Server	
Name*	
○ Server Name ● Server IP	
IP Address	
Port	
Time-out (seconds)	
Secret Key*	
Confirm Secret Key*	
Send Calling Station ID Details	
Create	

項目	値
Name	NetAttest_EPS
IP Address	192.168.1.2
Port	1812
Secret Key	secret

[NetScalar Gateway]-[Policies]-[Authentication]-[RADIUS]より「Policies」タブの「Add」をク リックします。

「Name」を入力し、「Server」で先ほど作成した RADIUS サーバーを選択します。「Expression」 において「ns true」を入力し、「Create」をクリックします。

Dashboard Configuration Reporting	Documentation	Downloads	\$
← Back			•
Create Authentication RADIUS Policy			
Name*			
NetAttest_EPS	ivpression Editor		
Operators Saved Policy Expressions Frequently Used Expressions Frequently Used Expressions	Clear		
Create Close			
項目			

Name	NetAttest_EPS_Policy
Server	NetAttest_EPS を選択
Expression	ns_true

3-6セッションポリシーの設定

NetScalar でセッションの設定を行います。

[NetScalar Gateway]-[Policies]-[Session]より「Profiles」タブの「Add」をクリックします。

「Name」を入力し、「Security」タブの「Default Authorization Action」にチェックを入れ、「ALLOW」

を選択します。

Dashboard Configuration Reporting			Documentation	Downloads	۵
					0
Create NetScaler Gateway Session Profile					
Name*					
Global NetScaler Gateway Parameters. Network Configuration Client Experience Security Public	ished Applications				
Default Authorization Action* ALLOW Image: Constraint of the second					
Create Close		J			
項目	値				
Name	NetAttes	stEPS_SessionProfile			
Default Authorization Action	ALLOW		1		

続いて「Published Applications」タブの「ICA Proxy」をチェックし、「OFF」を選択します。 「Create」をクリックします。

Network Configuration	Client Experience	Security	Published Applications
	Override G	Jobal	
ICA Proxy*			
Web Interface Address			
Web Interface Address Type	*		
IPV4			
Web Interface Portal Mode"			

[NetScalar Gateway]-[Policies]-[Session]よより「Policies」タブの「Add」をクリックします。 「Name」を入力し、「Action」で先ほど作成した「Session Profile」を選択します。「Expression」 において「ns_true」を入力し、「Create」をクリックします。



Virtual Server の設定

[NetScalar Gateway]-[Virtual Servers]より「Add」をクリックします。

「Name」、「IPAddress」、「Port」を入力し、「Continue」をクリックします。

Dashboard	Configuration	Reporting	De	ocumentation	Downloads	\$
+ Back						
VPN Virtual	Server			Help		>
Basic Settin Name* □ IPAddress* □ Port* 443 ► More Continue	gs Cancel	0 1 Pr-6				
項目	値					
Name	Ne	tAttest EPS Vserver]			

Name	NetAttest_EPS_Vserver
IPAddress	192.168.3.10
Port	443

続いて、「Certificates」において NetScalar にインポートされたサーバー証明書と CA 証明書を紐付けます。

ashboard Configuration	Reporting		Docu	mentation	Downloads	\$
← Back						
PN Virtual Server				Help		>
Basic Settings			/			
Name test IPAddress 192.168.3.12 Port 443	Max Users Max Login Attempts Failed Login Timeout State true ICA Only false Enable Authentication true	Double Hop Down State Flush AppFlow Logging ICA Proxy Session Migration Enable Device Certificate	false false false false false			
Certificates						
No Server Certificate			>			
No CA Certificate			>			
Continue						

サーバー証明書、CA 証明書ともに「Bind」をクリックし NetScalar にインポートされた証明書を選択し、「Save」をクリックします。その後「Continue」をクリックします。

Da	shboard	Configuration	Reporting		Documentation	Downloads	\$
4	Back		Server Cert Key				
			Server Cert Key				×
VF	PN Virtual S		Bind Unbind				
			Certificate	Server Certificate for SNI			
			No items				
			Save				

Dashboard Configuration	Reporting	Doc	umentation	Downloads	۵	
+ Back	CA Cert Key					
	CA Cert Key					×
VPN Virtual Server	Bind Unbind					
Basic Settings	Certificate	Check	Skip CA			
Name test	No items					
IPAddress 192.168.3.12 Port 443	Save					

続いて「Authentication」の右上の「+」をクリックします。

「Choose Type」で「RADIUS」を選択します。その後「Continue」をクリックします。

Authentication	+
To add, please click on the + icon	
Continue	

← Back	Choose Type		×
VPN Virtual Server	Policier		
Basic Settings	Class D F t		
Name test IPAddress 192.168.3.12 Port 443	LOCAL Choose Type* Primary Continue	Cancel	
項目	値		
Choose Type	RADIUS		

続いて「SSL Parameters」の右上のペンアイコンをクリックします。

「Client Authentication」にチェックし、「Save」をクリックします。

SSL Parameters					1
Enable DH ParamDISABLEDEnable Ephemeral RSAENABLEDRefresh Count0Enable Session ReuseENABLEDTime-out120SSL RedirectDISABLED	Clear Text Port Enable Cipher Redirect Client Authentication Send Close-Notify PUSH Encryption Trigger SNI Enable	0 DISABLED DISABLED YES Always DISABLED	SSLv2 Redirect SSLv2 SSLv3 TLSv1 TLSv11 TLSv11 TLSv12	DISABLED DISABLED ENABLED ENABLED ENABLED ENABLED	
SSL Parameters					
 Enable DH Param Enable Ephemeral RSA Refresh Count 0 		 SSL Redirect SNI Enable ✓ Send Close-Notify Clear Text Port 			
Enable Session Reuse Time-out 120 Enable Cipher Podirect		PUSH Encryption Trigger	Y		
Schull Radiract					
Protocol					
Protocol SSLv2 SSLv3 TLSv1	TLSv11 TLS	v12			

続いて「Policies」の右上の「+」をクリックします。

何も変更せずにそのまま「Continue」をクリックします。

その後、「Bind」をクリックし、[3-6 セッションポリシーの設定]にて作成したポリシーを選択します。「OK」をクリック後、「Done」をクリックします。

Policies	+ ×
Request Policies	
4 Cache Policies	>
Done	

SSL Parameters	Choose Type		-
	Choose Type		×
Enable Ephemeral RSA	Policies		
	Choose Policy*		
	Session 🗸		
Enable Session Reuse	Choose Type*		
	Request V		
	Request		
	Continue Cancel		
	Choose Type		
NetScaler (5550)	Choose Type		×
Dashboard Configuration	Policies		
4 Pack			
	Choose Policy	Choose Type	
	Session	Kequest	
	Bind Unbind Regenerate Priorities Edit Policy Edit Action		Search 🔻
	Priority Policy Name	Expression	Action
	No items		
	OK Close		

4. VPN クライアントの設定

4-1PC へのデジタル証明書のインストール

PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書 (user01_02.p12)をダブルクリックすると、証明書インポートウィザードが実行されます。





パスワード	
セキュリティを維持するために、	秘密キーはパスワードで保護されていました。
秘密キーのパスワードを入力	してください。
パスワード(円):	
□ 秘密キーの保護を強 このオブションを有効は	力にする(E) ですると、秘密キーがアプリケーションで使われるたびに確認を求められます。
このキーをエクスポート キーのバックアップやトラ	可能にする(M) ランスポートを可能にします。
-	< 戻る(B) 次へ(N) > キャンセル
-	
明書のインボート ウィザード	X
証明書ストア	
証明書ストバは、証明書から	米管されるシステム上の領域です。
	ストア(に配置する(円)
正明書ストア:	メトアに配置する(P) 参照(R)
正明書ストア:	<トバに配置する(L) 参照(B). 参照(B).
i 延 / 皆 C / (//////////////////////////////	<下/1.11 </th
■	< 、 、 、 、 、 、 、 、 、 、 、 、 、
■	ペアル(配置するむ) 参照(B). 《 戻る(B) 次へ(W) キャンセル ※ 証明書のインポート ウィザードの完了
正明書ストア:	
正明書ストア:	★ドハに配置するセ) ◆照(R). ◆原(R). ◆ (R).
正明書ストア:	
■	本外化配置するセン 参照(P). < 戻る(P)
■ 副用書ストア: ■ 用書のインポートウィザード	< 戻る(型)
■ 副 副 日 書 の インボートゥィザード 日 書 の インボートゥ イザード	< 戻る(B)
IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	< 戻る(型) 次へ(型) キャンセル
■	< 戻る(2)
ВШЯВДК?: ■ ПВО1ンポートウィザード	< 戻る(B)

【パスワード】 NetAttest EPS で証明書を 発行した際に設定したパスワードを入力

4-2NetScalar Gateway Plug-in のインストール

NetScalar Gateway にアクセスします。External 側のアクセス URL は「https://192.168.3.10/」 です。

Windows 端末で NetScalar Gateway に初回アクセス行うと、NetScalar Gateway Plug-in のダウ ンロード画面が表示されます。NetScalar Gateway Plug-in をダウンロードし、インストールを行 います。

TRIX NetScaler Gateway	
NetScaler Gateway	
NetScaler Gateway Plug-in がインストールされていない場合は、「 ダウンロード 」をクリックするとソフトウェアがインストールされ、自動的に接続します。	
プロキシ サーバーが設定されている場合は、Web ブラウザーのプロキシ例外に "localhost" を追加する必要があります。 詳しくは、ヘルプ デスクまだはシステム管理者に問い合わせてください。 ↓ダウンロード	
NetScaler Gateway Plug-in for Windows をインストールするいコま	
1. ビダウンロード 「をクリックします。	
2. [ファイルのダウンロード]ダイアログボックスで、[実行]をクリックします。	
3. プラウザー ダイアログボックスで、 [実行] をクリックして NetScaler Gateway Plug-In for Windows をインストールします。	



5. 接続テスト

NetScalar Gateway Plug-in がインストールされている端末で、ブラウザを利用して VPN 接続を行います。ブラウザより「https://192.168.3.10/」にアクセスします。

すると、クライアント証明書の提示を求められますので、[4-1 PC へのデジタル証明書のインストール]でインストールしたクライアント証明書を選択し、「OK」をクリックします。。



証明書認証に成功すると、以下の画面が表示されます。

[2-3 認証ユーザーの追加登録]にて NetAttest EPS に登録したユーザーID、パスワードを入力し、 「ログオン」をクリックします。



ログインに成功し、以下の画面が表示されますと、アクセス完了です。

A CONTRACTOR OF		
< 🕞 🖸 http://192.168.3.10:8080/vpns/portal/home 🔎 + 🖒 🛅	NetScaler Gateway 🛛 🗙 📈 RADIUS認証ログの表示 [シ	ሰ 🕁 🤁
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)) ()	
CITRIX' NetScaler Gateway		
		D747
Ping	Web ታብ	7ァイル共有
E24 次のビント NetScaler Gateway トンネルを通過するネットワークトラ フィッグは暗号化されます。	企業 Web サイト なし 個人 Web サイト なし 適加 副数	企業ファイル共有 なし 個人ファイル共有 なし 追加1利5%
ヘルフ ユーザーガイド		
		a 100% •



改訂履歴

日付	版	改訂内容
2013/10/08	1.0	初版作成