

NetScaler® セキュア展開ガイド

Contents

NetScaler MPX™、VPX、および SDX セキュリティのベストプラクティス	5
追加情報リソース	5
展開ガイドライン	6
物理セキュリティのベストプラクティス	6
NetScaler アプライアンスを安全な場所に展開する	6
NetScaler のフロントパネルとコンソールポートへのアクセスを保護する	6
電源保護	6
暗号鍵の保護	6
NetScaler セキュリティのベストプラクティス	7
NetScaler ソフトウェアの更新を実行する	7
NetScaler VPXをホストするサーバーのオペレーティングシステムを保護する	7
NetScalerのLOM（Lights Out Management）をリセットする	7
永続データの保守と削除	8
構成ガイドライン	8
ネットワークセキュリティ	8
主要なネットワークセキュリティの考慮事項	9
その他のネットワークセキュリティに関する考慮事項	10
NetScaler®でのパススルー通信の保護	18
管理	26
システムアカウントとユーザーアカウント	27
ロギングと監視	36
ネットワークタイムプロトコルを構成する	36
SNMPを構成する	36
外部NetScalerログホストへのロギングを構成する	37
セキュアチャネルを介したメッセージのエクスポートを設定する	38
LOM の構成	38

アプリケーションとサービス	39
NetScaler® を構成してアップグレードヘッダーを削除または渡す	39
無効なHTTPリクエストを破棄するようにNetScalerを構成する	40
HTTPサービス拒否攻撃に対する保護を構成する	41
TCPスプーフィング攻撃から防御するようにNetScalerを構成する	42
RFC 5961準拠を構成する	42
特定のHTTPヘッダーを受け入れるようにNetScalerを構成する	42
HTTPヘッダーのヘッダーサイズを構成する	43
NetScalerでのURLの正規化	43
強化されたTCP ISN生成	44
close-notifyの構成	45
管理GUI、NITRO API、およびRPC通信の保護	45
DNSSEC セキュリティに関する推奨事項	45
KSK/ZSK 秘密鍵には RSA 1024 ビット以上を使用する	46
DNSSEC キーの有効期限切れに対する SNMP アラームを有効にする	46
x.509 証明書の有効期限が切れる前に KSK/ZSK 秘密鍵をロールオーバーする	46
DNSSEC ADNS サーバーを保護する	46
レガシー構成	48
NetScaler®で暗号リダイレクトを無効にするように構成する	48
NetScalerでSSL再ネゴシエーション設定を構成する	48
NDcPP準拠証明書チェックの設定	49
NetScaler® 暗号化に関する推奨事項	49
TLS証明書とキーの管理	50
FIPSおよびNDcPP展開向けTLS暗号スイートの構成	50
NetScaler -FIPS の推奨事項	52
FIPSベースの展開におけるNetScaler SDXの構成	52
HSMパスワードを安全な場所に保管する	52
その他の機能	53

NetScaler® Web App Firewall セキュリティに関する推奨事項	53
NetScaler をツーマームモードで展開する	53
'Default Deny' ポリシーを使用する	53
NetScaler Web App Firewall – 複数のセキュリティ層を構築する	54
NetScaler® Gateway のセキュリティに関する推奨事項	56
「デフォルト拒否」ポリシーを使用する	56
サーバー間で TLS1.2 通信を使用する	57
イントラネットアプリケーションを使用する	57
認証、承認、および監査のセキュリティに関する推奨事項	57
NetScaler® Consoleセキュリティのベストプラクティス	61
NetScaler Console IPアドレスとNetScalerエージェントIPアドレスをインターネットに公開しないでください	61
システムユーザー向けの強力なパスワード	61
デフォルトの証明書を変更する	62
ローカル認証を無効にする	62
fix	64

NetScaler MPX™、VPX、および SDX セキュリティのベストプラクティス

NetScaler MPX は、Web サイトを高速化し、L4-L7 トラフィック管理を提供し、統合された NetScaler Web App Firewall を提供し、サーバーの負荷を軽減するアプリケーションデリバリーコントローラーです。NetScaler VPX インスタンスは、NetScaler MPX のすべての機能を備え、標準サーバー上で動作し、Citrix Virtual Apps and Desktops を含む Web アプリケーションの可用性を高める仮想アプライアンスです。NetScaler SDX は、VPX のすべての柔軟性と MPX のパフォーマンスを備えた高度な仮想化を提供します。MPX、VPX、および SDX を使用することで、組織は、大量の共有ネットワークサービスをプロセッサ負荷の高いアプリケーション固有のサービスから分離することにより、Web アプリケーション配信インフラストラクチャを最適化するフレックスまたは真のマルチテナンシーソリューションを展開できます。NetScaler はまた、Citrix OpenCloud Access とのシームレスな統合を提供し、クラウドの力でデータセンターを拡張できます。

展開ライフサイクル全体でセキュリティを維持するために、以下の考慮事項を確認することをお勧めします。

- 物理的セキュリティ
- アプライアンスセキュリティ
- ネットワークセキュリティ
- 管理と運用

展開の種類によって、セキュリティに関する考慮事項が異なる場合があります。このドキュメントでは、特定のセキュリティ要件に基づいて適切なセキュアな展開を決定するのに役立つ一般的なセキュリティガイダンスを提供します。

追加情報リソース

NetScaler® および NetScaler Gateway に関するその他のセキュリティ情報については、以下のリソースを参照してください。

- [セキュリティポータル](#)
- [製品ドキュメント](#)

NetScaler の構成に関する詳細なサポートについては、[<https://www.citrix.com/support.html>](https://www.citrix.com/support.html) でサポートリクエストを送信できます。

展開ガイドライン

NetScaler を展開する際は、以下の物理的およびアプライアンスのセキュリティに関するベストプラクティスを考慮してください。

物理セキュリティのベストプラクティス

NetScaler アプライアンスを安全な場所に展開する

NetScaler アプライアンスは、不正アクセスから NetScaler を保護するために、十分な物理的アクセス制御を備えた安全な場所に展開する必要があります。最低限、サーバールームへのアクセスは、鍵、電子カードリーダー、またはその他の同様の物理的方法で制御する必要があります。

その他の対策としては、部屋の活動を継続的に監視するために、CCTVなどの電子監視システムを使用することが挙げられます。不正侵入が発生した場合、このシステムからの出力はセキュリティ担当者に通知する必要があります。CCTVがある場合、記録された映像は監査目的で利用できません。

NetScaler のフロントパネルとコンソールポートへのアクセスを保護する

NetScaler または VPX ホスティングサーバーは、適切な鍵またはその他の物理的方法でロックできるラックまたはケージに展開する必要があります。このロックにより、NetScaler の物理ポート、または VPX 展開の場合は仮想化ホストコンソールへのアクセスが防止されます。

電源保護

NetScaler (またはホスティングサーバー) は、適切な無停電電源装置で保護する必要があります。停電が発生した場合、無停電電源装置は NetScaler の継続的な動作を保証するか、物理または仮想 NetScaler の制御されたシャットダウンを可能にします。無停電電源装置の使用は、電力サージに対する保護にも役立ちます。

暗号鍵の保護

展開で暗号鍵に追加の保護が必要な場合は、FIPS 140-2 レベル 2 準拠の NetScaler の使用を検討してください。FIPS プラットフォームは、ハードウェアセキュリティモジュールを使用して、NetScaler 内の重要な暗号鍵を不正アクセスから保護します。

NetScaler セキュリティのベストプラクティス

NetScaler ソフトウェアの更新を実行する

展開前に、お客様は NetScaler が最新のファームウェアバージョンに更新されていることを確認することをお勧めします。リモートで実行する場合は、SFTP や HTTPS などの安全なプロトコルを使用して NetScaler をアップグレードすることをお勧めします。

お客様は、NetScaler製品に関連するセキュリティ速報も確認することをお勧めします。新規および更新されたセキュリティ速報については、NetScalerセキュリティ速報のWebページ

[<https://support.citrix.com/knowledge-center/search#/>](https://support.citrix.com/knowledge-center/search#/) を参照し、新規および更新された速報のアラートに登録することを検討してください [<https://support.citrix.com/user/alerts>](https://support.citrix.com/user/alerts)。

NetScaler VPXをホストするサーバーのオペレーティングシステムを保護する

NetScaler VPXは、標準の仮想化サーバー上の仮想アプライアンスとして、またはNetScaler SDX上の仮想アプライアンスとして実行できます。

通常の物理セキュリティ手順を適用することに加えて、ロールベースのアクセス制御と強力なパスワード管理によって仮想化ホストへのアクセスを保護する必要があります。また、サーバーは、利用可能になった時点でオペレーティングシステムの最新のセキュリティパッチで更新され、仮想化の種類に適用できる場合は、最新のウイルス対策ソフトウェアをサーバーに展開する必要があります。NetScaler VPXをホストするためにNetScaler SDXプラットフォームを使用しているお客様は、NetScaler SDXの最新のファームウェアバージョンを使用していることを確認する必要があります。

NetScalerのLOM（Lights Out Management）をリセットする

本番環境での使用のためにLOMを設定する前に、LOMを工場出荷時の設定にリセットすることをお勧めします。

1. NetScalerシェルプロンプトで、次のコマンドを実行します。

```
>ipmitool raw 0x30 0x41 0x1
```

注記：

このコマンドを実行すると、LOMが工場出荷時のデフォルト設定にリセットされ、すべてのSSL証明書が削除されます。LOMポートを再構成する方法については、「[NetScaler MPXアプライアンスのLights Out Managementポート](#)」を参照してください。

2. LOM GUIで、**Configuration > SSL Certification** に移動し、証明書と秘密鍵を追加します。

また、LOM GUIを使用して以下のユーザー設定を行うことをお勧めします。

- **Configuration > Users > Modify User** に移動し、`nsroot` スーパーユーザーアカウントのパスワードを変更します。
- **Configuration > Users > Modify User** に移動し、ユーザーのポリシーを作成するか、既存のポリシーをユーザーにバインドします。
- **Configuration > IP Access Control > Add** に移動し、既知のIPアドレス範囲へのアクセスを許可するようにIPアクセス制御を設定します。
- **Configuration > Users > Modify User** に移動し、代替のスーパーユーザーアカウントを作成し、このアカウントにポリシーをバインドします。

LOM構成の詳細については、[LOM Configuration](#)を参照してください。

永続データの保守と削除

NetScalerが別の環境に再展開された場合、廃止された場合、またはRMAで返却された場合、永続データがNetScalerから正しく削除されていることを確認してください。

このプロセスの詳細については、[Wiping your data before sending the ADC appliance to Citrix](#)を参照してください。

構成ガイドライン

NetScaler を構成する際は、以下の構成ガイドラインを考慮してください。

- ネットワークセキュリティ ([/ja-jp/netScaler-adc-secure-deployment/configuration-guidelines/network-security.html](#))
- NetScaler でのパススルー通信の保護 ([/ja-jp/netScaler-adc-secure-deployment/configuration-guidelines/securing-pass-through-traffic-on-netScaler.html](#))

ネットワークセキュリティ

NetScalerを本番環境に展開する際には、以下の主要な構成変更を行うことをお勧めします。

- NetScaler管理者インターフェース (NSIP) をインターネットに公開しないでください。
- NetScalerのデフォルトSSL証明書は置き換える必要があります。
- GUIにアクセスする際はHTTPS (HTTP over TLS) を使用し、デフォルトのHTTPインターフェースは無効にする必要があります。

以下のセクションでは、これらの主要な考慮事項に加え、推奨されるさらなる変更点について詳しく説明します。

主要なネットワークセキュリティの考慮事項

NSIPおよび管理サービスIPアドレスをインターネットに公開しないでください:

NetScaler管理IP（NSIP）アドレスおよびSDXの管理サービスIPアドレスは、パブリックインターネットに公開せず、適切なステートフルパケットインスペクション（SPI）ファイアウォールの背後に展開することをお勧めします。

NetScalerのデフォルトTLS証明書を置き換える:

NetScalerの初期設定中に、デフォルトのTLS証明書が作成されます。これらの証明書は本番環境での使用を意図したものではなく、置き換える必要があります。

お客様は、信頼できる認証局（CA）からの証明書、または企業認証局からの適切な証明書を使用するようにNetScalerを設定することをお勧めします。

公開仮想サーバーにバインドされている場合、信頼できるCAからの有効なTLS証明書は、インターネットに公開されているWebアプリケーションのユーザーエクスペリエンスを簡素化します。ユーザーのWebブラウザは、Webサーバーとの安全な通信を開始する際にユーザーの操作を必要としません。NetScalerのデフォルト証明書を信頼できるCA証明書に置き換えるには、Knowledge Centerの記事CTX122521: [「アプライアンスのホスト名と一致する信頼できるCA証明書でNetScalerアプライアンスのデフォルト証明書を置き換える方法」](#)を参照してください。

あるいは、カスタムTLS証明書と秘密鍵を作成して使用することも可能です。この操作は同等のトランスポート層セキュリティを提供できますが、TLS証明書をユーザーに配布する必要があり、Webサーバーへの接続を開始する際にユーザーの操作が必要となります。カスタム証明書の作成方法の詳細については、Knowledge Centerの記事CTX121617: [NetScalerアプライアンスで自己署名証明書を作成およびインストールする方法](#)を参照してください。

TLS証明書の管理と構成に関する詳細情報は、このガイドの「NetScaler TLSの推奨事項」セクションで確認できます。

管理者インターフェースへのHTTPアクセスを無効にする:

NetScaler管理インターフェースおよびGUIへのトラフィックを保護するために、NetScalerはHTTPSを使用するように構成する必要があります。次の手順を実行します。

- 2048ビット以上のRSA秘密鍵と公開鍵のペアを作成し、HTTPSおよびSSHでNetScaler IPアドレスにアクセスするためにその鍵を使用します。工場出荷時にプロビジョニングされた512ビットのRSA秘密鍵と公開鍵のペアは置き換えてください。

- NetScalerが強力な暗号スイートのみを使用するように構成し、NetScalerの「DEFAULT」暗号スイートセットを強力な暗号スイートに変更します。NIST Special Publication 800-52 (Revision 1) のセクション3.3に記載されている承認済みTLS暗号スイートのリストを使用することをお勧めします。このドキュメントは、NISTのWebサイトで次のアドレスから入手できます: https://www.nist.gov/publications/guidelines-selection-configuration-and-use-transport-layer-security-tls-implementations?pub_id=915295
- 管理者インターフェースにアクセスするために、NetScalerがSSH公開鍵認証を使用するように構成します。NetScalerのデフォルトキーは使用しないでください。独自の2048ビットRSA秘密鍵と公開鍵のペアを作成して使用してください。詳細については、Knowledge Centerの記事CTX109011: [公開鍵認証でNetScalerアプライアンスへのSSHアクセスを保護する方法](#) およびNetScaler製品ドキュメント: [ローカルシステムユーザー向けのSSHキーベース認証](#) を参照してください。
- NetScalerがこれらの新しい証明書を使用するように構成されたら、次のコマンドでGUI管理インターフェースへのHTTPアクセスを無効にできます。

```
set ns ip <NSIP> -gui SECUREONLY
```

その他のネットワークセキュリティに関する考慮事項

SDXの管理を信頼されていないVPX管理者のVPXシェルアクセスを制限する:

Management Serviceの管理者とは異なる人物がVPXを管理することが望ましい状況では、Management Service管理者は、VPX上でシェルアクセスが制限されたVPX管理者ユーザーを作成し、その制限された管理者ユーザーアカウントのみをVPX管理者に提供する必要があります。

一部の操作（SSL証明書の管理など）にはシェルアクセスが必要な場合があります。ただし、SVMの管理を信頼されている個人にのみ、VPXインスタンスシェルへのアクセスを許可する必要があります。このセクションの後半に記載されているRBACレベルのコマンドは、これらのアカウントに割り当てることができます。これらの推奨事項は、すべてのSVM-IP/VPX-NSIP（L2/L3）管理ワークフローに適用され、セキュアなアクセス監査目的のために従う必要があります。

VPX管理者からシェルアクセスを削除するには、次の手順を使用できます。

既存のVPXインスタンスの保護:

1. `nsroot` またはスーパーユーザーとしてVPX CLIにログインします。

`nsroot` アカウントを使用せず、代わりにスーパーユーザーアカウントを作成することをお勧めします。 `nsroot` アカウントを使用する場合は、特殊文字を含む強力なパスワードであ

ることを確認してください。強力なパスワードの詳細については、[管理と運用](#) を参照してください。

- NetScaler SDX上のVPXインスタンスでユーザーとRBACポリシーを作成します。
- そのユーザーをポリシーにバインドします。

```
> add system user userabc

Enter password:

Confirm password:

Done

> bind system user userabc superuser 2

Done

> add system cmdpolicy shell deny (shell)

Done

> bind system user userabc shell 1

Done
```

注:

この例では、シェルアクセスを拒否するためにシステム `cmdpolicy` (例: `cmdpolicy` 名: `shell`) が作成されます。このポリシーは、優先度を高くしてユーザー `userabc` にバインドされます。デフォルトのスーパーユーザー `cmdpolicy` も、システムユーザーに低い優先度でバインドされます。この構成により、新しいシステムユーザーはスーパーユーザーRBACポリシーを持ちますが、シェルアクセスは拒否されます。

2. 新しいシステムユーザーとしてログインし、次のアクションを実行します。

- 現在のユーザーがRBACポリシーを適用していることを確認します。
- ユーザーが許可されているコマンドを実行します。(例: `show system cmdpolicy`)

- シェルアクセスが制限されていることを確認するために、`shell` コマンドを実行します。

ログイン名: `userabc`

サーバーからの事前認証バナーメッセージ:

```
|
#####
#####

> ##

| #

> #

| #      WARNING: Access to this system is for authorized users only

> #

| #      Disconnect IMMEDIATELY if you are not an authorized user!

> #

| #

> #

|
#####
#####

> ##

|

End of banner message from server

Keyboard-interactive authentication prompts from server:

| Password:
```

```
End of keyboard-interactive prompts from server
```

```
Last login: Thu May 13 04:11:15 2021 from 10.10.1.1
```

```
Done
```

```
> whoami
```

```
UserName: userabc
```

```
LoggedIn: "Thu May 13 04:18:50 2021"
```

```
Done
```

3. そのVPXのコンソールで、そのユーザーとしてログインし、このユーザーにはシェルアクセスが許可されていないことを確認します。

```
> shell
```

```
ERROR: Not authorized to execute this command [shell]
```

4. 通常の管理者ユーザー (`nsroot`) としてログインし、シェルアクセスが許可されていることを確認します。

```
> shell
```

```
Copyright (c) 1992-2013 The FreeBSD Project.
```

```
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,  
1994
```

```
The Regents of the University of California. All rights reserved.
```

```
root@Zela-40G-10#
```

新しいVPXインスタンスの保護:

1. 管理サービスGUIから新しいVPXインスタンスが作成される際、インスタンス管理者ユーザーを作成し、**Shell/SFTP/SCP Access** チェックボックスをオフにします。シェルアクセスを無

効にすると、`svm_access_policy` (アクション DENY) が指定されたインスタンス管理者ユーザーに明示的にバインドされます。

2. このユーザー情報をVPX管理者に提供します。SDX管理者は、この `nsroot` 管理者パスワードを保持し、VPX管理者と共有してはなりません。

注記

- `nsroot` パスワードを変更するには、Management Serviceにログオンし、インスタンスを選択してパスワードを変更します。VPX CLIから `nsroot` パスワードを変更しないでください。
- RBACユーザーの詳細については、[ユーザー、ユーザーグループ、およびコマンドポリシー](#)を参照してください。
- SVMからNetScalerのパスワードを変更する方法については、[NetScalerインスタンスの変更](#)を参照してください。
- インスタンス管理でNetScalerをプロビジョニングする方法については、[NetScalerインスタンスの追加](#)を参照してください。

SSHポートフォワーディングを無効にする:

NetScalerではSSHポートフォワーディングは不要です。この機能を使用しない場合は、以下の手順で無効にすることをお勧めします。

1. 次の行を追加して、`/etc/sshd_config` ファイルを編集します。

```
AllowTcpForwarding no
```

2. ファイルを保存し、テスト中に再起動した場合でも変更が永続的になるように、`/nsconfig` ディレクトリにコピーします。
3. 次のコマンドを使用して、`sshd` プロセスを再起動します。

```
kill -HUP `cat /var/run/sshd.pid`
```

NetScalerを高可用性で構成する:

継続的な運用が必要な展開では、NetScalerを高可用性セットアップで展開できます。このようなセットアップは、NetScalerのいずれかが機能しなくなったり、オフラインアップグレードが必要になったりした場合でも、継続的な運用を提供します。

高可用性セットアップの構成方法については、[高可用性の構成](#)を参照してください。

ピアアプライアンス間のセキュアな通信を設定する:

NetScalerを高可用性、クラスター、またはGSLBセットアップで構成している場合は、NetScalerアプライアンス間の通信を保護してください。

通信を保護するために、内部ユーザーアカウントまたはRPCノードのパスワードを変更し、**Secure**および****validateCert****オプションを有効にすることをお勧めします。RPCノードは、構成およびセッション情報のシステム間通信に使用される内部システムエンティティです。**-validateCert** オプションは、ノード間の構成同期や構成伝播などのRPC通信におけるサーバー証明書の検証を可能にします。

```
set ns rpcNode <IP> -secure ON -validateCert YES
```

-validateCert オプションは、**-secure** パラメーターが **ON** に設定されている場合にのみ有効です。

サーバー証明書を検証するには、CA `/nsconfig/ssl/certs/ca.pem` ファイルを構成する必要があります。したがって、`nsrpcs-127.0.0.1-3008` サービス用のサーバー証明書の署名に使用されるピアCA証明書でCAファイル `/nsconfig/ssl/certs/ca.pem` を構成してください。詳細については、[RPCノードのパスワードを変更する](#)を参照してください。

NetScalerの機能は、内部ユーザーアカウントが無効になっている場合、内部通信にSSHキーベースの認証を使用することもできます。そのような場合、キー名は「ns_comm_key」に設定する必要があります。詳細については、[SSHキーを使用してパスワードなしでNetScalerアプライアンスにアクセスする](#)を参照してください。

デフォルトのパスワードを変更する:

セキュリティを強化するために、オンプレミスおよびクラウド展開の両方で、管理者、内部ユーザーアカウント、またはRPCノードのパスワードを変更することをお勧めします。パスワードを頻繁に変更することが推奨されます。

- 管理者パスワード: [管理者パスワードを変更する](#)を参照してください。
- 内部ユーザーアカウントまたはRPCノードのパスワード: [RPCノードのパスワードを変更する](#)を参照してください。

注

また、内部ユーザーアカウントを無効にし、代わりにキーベースの認証を使用することをお勧めします。

ネットワークセキュリティドメインとVLANを構成する:

NetScaler管理インターフェイスへのネットワークトラフィックは、物理的または論理的に、通常のネットワークトラフィックから分離することをお勧めします。推奨されるベストプラクティスは、3つのVLANを持つことです。

- 外部インターネットVLAN
- 管理VLAN
- 内部サーバーVLAN

LOMポートを管理VLANの一部にするようにネットワークを設定することをお勧めします。

NetScalerを2アームモードで展開する場合、特定のポートを特定のネットワークに割り当ててください。VLANタギングと2つのネットワークを1つのポートにバインドする必要がある場合は、2つのネットワークが同じ、または類似したセキュリティレベルであることを確認する必要があります。

2つのネットワークのセキュリティレベルが異なる場合、VLANタギングは使用しないでください。代わりに、特定のネットワークごとにポートを割り当て、NetScalerのポート全体に分散された独立したVLANを使用することを検討してください。

NetScaler Web App Firewallの使用を検討してください: Premium EditionライセンスのNetScalerは、ポジティブセキュリティモデルを使用し、コマンドインジェクション、SQLインジェクション、クロスサイトスクリプティングなどの脅威から保護するために適切なアプリケーション動作を自動的に学習する組み込みのNetScaler Web App Firewallを提供します。

NetScaler Web App Firewallを使用すると、ユーザーはコードの変更なしに、また最小限の設定変更でWebアプリケーションにさらなるセキュリティを追加できます。詳細については、

「[NetScaler Web Application Firewallの概要](#)」を参照してください。

非管理アプリケーションのアクセスを制限する: 非管理アプリケーションがNetScalerにアクセスする機能を制限するには、次のコマンドを実行します。

```
set ns ip <NSIP> -restrictAccess enabled
```

セキュアなクラスター展開:

クラスター展開を保護するために、ネットワーク攻撃に対する保護を提供するセキュアハートビート機能を有効にすることをお勧めします。

注:

セキュアハートビート機能は、NetScalerリリース14.1ビルド12.x以降で利用可能です。

セキュアハートビート機能を有効にするには、クラスターIPアドレスにログインし、次のコマンドを実行します。

```
set cluster instance <clId> secureHeartbeats ENABLED
```

セキュアハートビート機能の詳細については、「[セキュアハートビートの設定](#)」を参照してください。

通信を保護するために、内部ユーザーアカウントまたはRPCノードのパスワードを変更し、**Secure**オプションと`**validateCert**`オプションを有効にすることをお勧めします。

```
set rpcnode <ip> -secure on -validateCert YES
```

注: その他の設定が必要になる場合があります。詳細については、「[製品ドキュメント](#)」の**クラスタリング**に関するトピックを参照してください。

L3クラスター展開で展開される場合、NetScalerノード間のパケットは、ルーティングのために送信元および宛先ノードのNSIPアドレスを使用する暗号化されていないGREトンネルを介して交換されます。インターネットを介して交換が行われる場合、IPsecトンネルがないと、NSIPがインターネットに公開されます。これは、NetScalerのセキュリティベストプラクティスに準拠していないため、推奨されません。

顧客がL3機能上でクラスターを使用するために、独自のIPsecソリューションを確立することをお勧めします。

IP転送機能を使用していない場合は、次のコマンドを使用してL3モードを無効にします。

```
disable ns mode L3
```

グローバルサーバー負荷分散 (GSLB) にセキュアなMEPを使用する: GSLB 用のNetScaler間の MEPを暗号化するには、NSCLI から次のコマンドを実行します。

```
set rpcNode <GSLB Site IP> -secure yes
```

負荷分散の永続性クッキーを保護する:

SSL/TLSチャネルに加えて、負荷分散の永続性クッキーを暗号化することをお勧めします。詳細については、[HTTPクッキーの永続性](#)を参照してください。

DTLS DDoS増幅攻撃を軽減するためのHelloverifyrequestパラメーター:

NetScaler リリース 12.1 ビルド 62.x およびリリース 13.0 ビルド 79.x 以降、

`helloverifyrequest` パラメーターはデフォルトで有効になっています。DTLS プロファイルで `helloverifyrequest` パラメーターを有効にすると、攻撃者やボットがネットワークスループットを圧倒し、アウトバウンド帯域幅の枯渇につながるリスクを軽減するのに役立ちます。つまり、DTLS DDoS 増幅攻撃を軽減するのに役立ちます。

`helloverifyrequest` パラメーターのステータスを表示するには、CLI プロンプトで次のように入力します。

```
show dtlsProfile
```

NetScaler®でのパススルー通信の保護

NetScalerでパススルー通信を保護するために、インフラストラクチャモード設定を使用できます。これらのインフラストラクチャモード設定は、アプリケーションを中断することなく、基本的なレベルのセキュリティを提供します。利用可能なインフラストラクチャモード設定の概要を以下に示します。

- セッション状態保護
- セッション固定保護 (HTTP Only を有効にする)
- HSTS (HTTP Strict Transport Security (HSTS) を有効にする)
- 強力な認証
- エンドツーエンドSSLを推奨
- HTTPSをプロキシ / その他のすべての通信を拒否

セッション状態保護:

推奨: 有効 NetScaler: ほとんどのエンティティでデフォルトで有効

セッション状態保護設定はデフォルトで有効になっており、特定の構成は必要ありません。NetScalerが接続をプロキシするように構成されている場合、たとえば、フローが構成された仮想サーバーまたはTCPタイプ以上のサービスを選択すると、NetScalerはステートフルセッションを作成します。NetScalerはこれらの接続の状態を維持し続け、このステートマシンに該当するパケットのみが処理されます。その他のパケットは破棄されるか、リセットされます。

以下のサービスタイプエンティティは、NetScalerでこのステートフルな動作を実現します。

- ADNS_TCP
- DIAMETER, DNS_TCP
- FTP-c
- GRE-c
- HTTP
- MYSQL, MSSQL
- NNTP
- ORACLE
- PUSH, PPTP
- RTSP, RDP
- SIP_SSL, SIP_TCP
- SMPP
- SSL, SSL_BRIDGE, SSL_DIAMETER, SSL_PUSH
- SSL_TCP, SYSLOG_TCP
- TCP
- ADNS_TCP
- RNAT (rnat_tcpproxy が有効になっている)

セッションフィクセーション保護 (HttpOnlyフラグを有効にするか、書き換えポリシーを追加することによって) :

推奨事項: NetScalerまたはバックエンドサーバーによって設定されたCookieに対してHttpOnlyを有効にするにはNetScaler: NetScalerが挿入するCookieについてはデフォルトで有効。バックエンドサーバーによって設定されたCookieについてはリライト経由で可能。

HttpOnly: CookieにHttpOnlyフラグを付けると、そのCookieはサーバーのみがアクセスできることをブラウザに示します。クライアントスクリプトからCookieにアクセスしようとする試みは厳しく禁止されます。HttpOnly Cookieは、適切に実装されていれば、一般的なクロスサイトスクリプティング攻撃の大部分をはるかに困難にします。

以下は、HttpOnlyフラグが設定されたCookieの例です。

```
Set-Cookie: ASP.NET_SessionId=ig2fac55; path=/; HttpOnly
```

Cookie挿入永続性のためにNetScalerによって挿入されるCookieは、デフォルトでHttpOnlyフラグを設定し、そのCookieがスクリプト不可能であり、クライアントアプリケーションに開示されてはならないことを示します。したがって、クライアント側のスクリプトはCookieにアクセスできず、クライアントはクロスサイトスクリプティングの影響を受けません。

コマンドラインインターフェイスを使用してHttpOnlyフラグ設定を有効にするには：

コマンドプロンプトで、次のように入力します。

```
set lb parameter -HttpOnlyCookieFlag (ENABLED)
```

リライトポリシーを使用してCookieにSecureとHttpOnlyを挿入する：

リライトポリシーは、バックエンドサーバーから送信されるCookieに対してSecureとHttpOnlyを挿入します。

注： SecureおよびHttpOnly Cookieは、SSL VIPに対してまとめて設定できます。非SSL VIPの場合、HttpOnlyフラグを挿入できます。

NetScalerを使用すると、サーバーによって設定されたCookieに対してHttpOnlyフラグとSecureフラグを含めることができます。

- HttpOnly - Cookieのこのオプションにより、WebブラウザはHTTP（またはHTTPS）プロトコルのみを使用してCookieを返します。JavaScriptのdocument.cookie参照などの非HTTPメソッドはCookieにアクセスできません。このオプションは、クロスサイトスクリプティングによるCookieの盗難を防ぐのに役立ちます。
- Secure - Cookieのこのオプションにより、WebブラウザはSSLによって送信が暗号化されている場合にのみCookie値を返します。このオプションは、接続の盗聴によるCookieの盗難を防ぐために使用できます。

CLIを使用してリライトポリシーを作成する

1. リライト機能がまだ有効になっていない場合は、有効にします。

```
enable feature REWRITE
```

2. リライトアクションを作成します（この例では、SecureフラグとHttpOnlyフラグの両方を設定するように構成されています。どちらか一方が欠けている場合は、他の組み合わせに合わせて必要に応じて変更してください）。

```
add rewrite action <action name> replace_all http.RES.full_Header  
 "\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\\; Secure;  
 HttpOnly)|(path=/\\; Secure)|(path=/\\; HttpOnly)|(path=/)!)"  
 -bypassSafetyCheck YES
```

例:

```
add rewrite action act_cookie_Secure replace_all http.RES.full_Header  
 "\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\\; Secure;  
 HttpOnly)|(path=/\\; Secure)|(path=/\\; HttpOnly)|(path=/)!)"
```

or

```
add rewrite action act_cookie_Secure replace_all http.RES.full_Header  
 "\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\\; Secure;  
 HttpOnly)|(path=/\\; Secure)|(path=/\\; HttpOnly)|(path=/)!)"  
 -bypassSafetyCheck YES
```

注:

NetScaler リリース 13.1 以降、 `bypassSafetyCheck` パラメータは適用されません。ただし、13.1 より前のリリースでは、このパラメータはサポートされています。

3. アクションをトリガーするリライトポリシーを作成します。

```
add rewrite policy <policy name> "http.RES.HEADER(\"Set-  
 Cookie\").EXISTS" <action name>
```

例:

```
add rewrite policy rw_force_secure_cookie "http.RES.HEADER(\"Set-Cookie\").EXISTS" act_cookie_Secure
```

4. 保護する仮想サーバーにリライトポリシーをバインドします (Secure オプションを使用する場合は、SSL 仮想サーバーを使用する必要があります)。

```
bind lb vserver <vserver name> - <policy name> -priority <priority number> -gotoPriorityExpression NEXT -type RESPONSE
```

例:

```
bind lb vserver mySSLVServer -policyName rw_force_secure_cookie -priority 100 -gotoPriorityExpression NEXT -type RESPONSE
```

詳細については、[<https://support.citrix.com/article/CTX138055>](https://support.citrix.com/article/CTX138055) を参照してください。

HSTS (HTTP Strict Transport Security (HSTS) を有効にする):

NetScaler コマンドラインを使用して HSTS を有効にするには:

コマンドプロンプトで、次のように入力します。

```
set ssl vserver <vServerName> -HSTS ( ENABLED ) maxage <positive_integer> -IncludeSubdomains ( YES | NO )
```

または

```
set ssl profile <name> -HSTS ( ENABLED ) -maxage <positive_integer> -IncludeSubdomains ( YES | NO )
```

詳細については、以下のトピックを参照してください。

- [HTTP Strict Transport Security \(HSTS\) のサポートを構成する。](#)
- [<https://support.citrix.com/article/CTX205221>](https://support.citrix.com/article/CTX205221)

強力な認証:

強力な認証（または多要素認証 – MFA）は、機密データ、アプリ、および管理へのすべてのアクセスに対して有効にする必要があります。

機密性の高いアプリを多要素認証用に設定する方法の詳細については、[多要素 \(nFactor\) 認証](#)を参照してください。

エンドツーエンドSSLを推奨:

フロントエンドとバックエンドの両方でSSLを使用することをお勧めします。SSLv3、TLS 1.0、TLS 1.1などの古い安全でないプロトコルバージョンは、SSLエンティティで無効にできます。TLS 1.2とTLS 1.3のみを有効にできます。これはSSLエンティティレベルまたはプロファイルレベルで実行でき、すべてのSSLエンティティはプロファイルからSSL設定を継承します。

CLIを使用して、SSLエンティティで安全でないプロトコルバージョンを無効にし、安全なプロトコルバージョンを有効にする

コマンドプロンプトで、次のように入力します。

```
set ssl vservice <vServerName> -ssl2 DISABLED -ssl3 DISABLED -tls1
DISABLED -tls11 DISABLED -tls12 ENABLED -tls13 ENABLED

set ssl service <vServiceName> -ssl2 DISABLED -ssl3 DISABLED -tls1
DISABLED -tls11 DISABLED -tls12 ENABLED -tls13 ENABLED
```

SSLプロファイルが有効になっている場合は、次のコマンドを使用します:

```
set ssl profile <frontend profile> -ssl3 DISABLED -tls1 DISABLED -
tls11 DISABLED -tls12 ENABLED -tls13 ENABLED

set ssl profile <backend profile> -ssl3 DISABLED -tls1 DISABLED -
tls11 DISABLED -tls12 ENABLED -tls13 ENABLED
```

****注:**

仮想サーバーエンティティで有効にするのではなく、プロファイルを使用してTLS 1.3を有効にすることをお勧めします。詳細については、[TLS 1.3プロトコルのサポート](#)を参照してください。

NetScalerが推奨する暗号スイート:

NetScalerがサポートする以下の暗号は、「必須破棄」リストのコンポーネントを含んでいません。これらの暗号は、鍵交換（RSA、DHE、およびECDHE）によって整理され、パフォーマンスの高いものが上部に、セキュリティの高いものが下部に配置されています。

推奨されるRSA鍵交換暗号スイート:

- TLS1-AES-128-CBC-SHA
- TLS1-AES-256-CBC-SHA
- TLS1.2-AES-128-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES256-GCM-SHA384

推奨されるDHE鍵交換暗号スイート:

- TLS1-DHE-RSA-AES-128-CBC-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1.2-DHE-RSA-AES-128-SHA256
- TLS1.2-DHE-RSA-AES-256-SHA256
- TLS1.2-DHE-RSA-AES128-GCM-SHA256
- TLS1.2-DHE-RSA-AES256-GCM-SHA384

推奨されるECDHE鍵交換暗号スイート:

- TLS1-ECDHE-RSA-AES128-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256

- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384

推奨される暗号スイート（優先順位順）：

以下の暗号リストには、RSA、DHE、およびECDHE鍵交換が含まれています。これは、セキュリティ、パフォーマンス、および互換性の間で最良の妥協点を提供します。

1. TLS1.2-AES128-GCM-SHA256
2. TLS1.2-AES-128-SHA256
3. TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
4. TLS1.2-ECDHE-RSA-AES-128-SHA256
5. TLS1-ECDHE-RSA-AES128-SHA
6. TLS1.2-DHE-RSA-AES128-GCM-SHA256
7. TLS1.2-DHE-RSA-AES-128-SHA256
8. TLS1-DHE-RSA-AES-128-CBC-SHA
9. TLS1-AES-128-CBC-SHA

SSLセキュアプロファイルとセキュア暗号：

セキュアフロントエンドプロファイル (ns_default_ssl_profile_secure_frontend) をSSL仮想サーバーにバインドすることをお勧めします。セキュアな暗号エイリアスが追加され、セキュアフロントエンドプロファイルにバインドされます。このエイリアスの一部である暗号を一覧表示するには、コマンドプロンプトで次のように入力します。

```
show cipher SECURE
```

```
1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1
```

```
          Description: TLS 1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)  
Mac=AEAD  HexCode=0xc030
```

```
2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2
```

```
          Description: TLS 1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)  
Mac=AEAD  HexCode=0xc02f
```

```
3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384  
Priority : 3
```

```

Description: TLS 1.2 Kx=ECC-DHE Au=ECDSA Enc=AES-GCM(256)
Mac=AEAD HexCode=0xc02c

```

```

4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
Priority : 4

```

```

Description: TLS 1.2 Kx=ECC-DHE Au=ECDSA Enc=AES-GCM(128)
Mac=AEAD HexCode=0xc02b

```

```

Done

```

セキュアフロントエンドプロファイルの詳細は、[セキュアフロントエンドプロファイル](#)を参照してください。

SSL内部サービスでは、TLS 1.2より低いプロトコルは無効になっています。デフォルト（拡張）プロファイルが有効になっている場合、ns_default_ssl_profile_internal_frontend_serviceプロファイルがSSL内部サービスにバインドされ、SSLv3、TLS 1.0、TLS 1.1、およびTLS 1.3プロトコルがプロファイルで無効になります。

プロキシHTTPS / その他のすべてのトラフィックを拒否:

可能な限り、セキュアなSSLバージョン（TLS 1.2またはTLS 1.3）とセキュアな暗号を使用して、データの暗号化を強化するためにSSL VIPを使用してください。VIPおよびバックエンドSSLサービスでSSLを有効にする際には、SSL TPSとSSLスループットを考慮する必要があります。

管理

このセクションでは、NetScalerおよびNetScaler SDXのセキュリティを強化するために適用できる特定の構成変更の例を示します。NetScaler構成のベストプラクティスに関する詳細なガイダンスは、記事「[NetScalerアプライアンスの一般的な実装に関する推奨設定とベストプラクティス](#)」で確認できます。

詳細については、以下のトピックを参照してください。

- [システムおよびユーザーアカウント](#)
- [ログと監視](#)
- [LOM構成](#)
- [アプリケーションとサービス](#)
- [DNSSECセキュリティに関する推奨事項](#)

- [レガシー構成](#)
- [NDCPP準拠証明書チェックの構成](#)

システムアカウントとユーザーアカウント

スーパーユーザーアカウントのパスワードを変更する: 組み込みの管理者スーパーユーザー (`nsroot`) は削除できません。そのため、そのアカウントのデフォルトパスワードを安全なパスワードに変更してください。管理者ユーザーのデフォルトパスワードを変更するには、次の手順を実行します。

1. スーパーユーザーとしてログオンし、構成ユーティリティを開きます。
2. ナビゲーションペインで、ノードを展開します。
3. ノードを選択します。
4. ページで、 `nsroot` ユーザーを選択します。
5. を選択します。
6. フィールドと フィールドに、必要なパスワードを入力します。
7. をクリックします。

代替スーパーユーザーアカウントを作成する: スーパーユーザーアカウントを作成するには、次のコマンドを実行します。

```
add system user <newuser> <password>

bind system user <newuser> superuser 0
```

デフォルトの `nsroot` スーパーユーザーアカウントの代わりに、このスーパーユーザーアカウントを使用してください。

NetScaler SDX展開の場合、管理者は初期設定後にNetScaler SDXとそのGUI管理コンソールのデフォルトの資格情報を変更する必要があります。デフォルトユーザーのパスワードを変更するには、次の手順を実行します。

1. スーパーユーザーとしてログオンし、構成ユーティリティを開きます。
2. ナビゲーションペインで、ノードを展開します。
3. ノードを選択します。
4. 「システムユーザー」 ページで、デフォルトユーザーを選択します。

5. 「変更」を選択します。
6. 「パスワード」フィールドと「パスワードの確認」フィールドに、必要なパスワードを入力します。
7. 「OK」をクリックします。

システムユーザーの強力なパスワード:

NetScalerで作成されたシステムユーザーアカウントには、強力なパスワードを使用することをお勧めします。パスワードの複雑さの要件の例は次のとおりです。

- パスワードは8文字以上の長さである必要があります。
- パスワードには、辞書に載っている単語や、辞書に載っている単語の組み合わせを含めてはなりません。
- パスワードには、少なくとも1つの大文字、1つの小文字、1つの数字、および1つの特殊文字を含める必要があります。

強力なパスワードは、パスワードの最小長とパスワードの複雑さを強制するための2つのパラメータを設定することで適用できます。

```
set system parameter -minpasswordlen <positive_integer> -  
-strongpassword ( ENABLED | DISABLED )
```

複数の管理者が要求される展開では、RADIUS、TACACS+、LDAP(S)などの外部認証方法を使用してユーザーを認証することを検討してください。詳細については、「[外部ユーザー認証](#)」を参照してください。

管理アクセス用のシステムユーザーアカウントのロック: NetScalerでは、システムユーザーを24時間ロックし、ユーザーへのアクセスを拒否できます。NetScalerは、システムユーザーと外部ユーザーの両方の構成をサポートしています。コマンドプロンプトで次のように入力します。

```
set aaa parameter -persistentLoginAttempts DISABLED
```

次に、ユーザーアカウントをロックするには、コマンドプロンプトで次のように入力します。

```
lock aaa user test
```

GUIを使用してこの機能を構成する方法については、「ユーザーアカウントとパスワード管理」を参照してください([/ja-jp/citrix-adc/current-release/system/authentication-and-authorization-for-system-user/user-account-and-password-management.html](#))。

管理アクセス用にロックされたシステムユーザーアカウントのロックを解除する: システムユーザーと外部ユーザーは、認証、承認、および監査ユーザーコマンドのロックを使用して24時間ロックできます。NetScalerを使用すると、ロックされたシステムユーザーのロックを解除できます。コマンドプロンプトで、次のように入力します。

`unlock aaa user test` GUIを使用してこの機能を構成する方法については、「ユーザーアカウントとパスワード管理」を参照してください(/ja-jp/citrix-adc/current-release/system/authentication-and-authorization-for-system-user/user-account-and-password-management.html)。

システムユーザーアカウントの管理アクセスを無効にする: NetScalerで外部認証が構成されており、管理アクセスへのシステムユーザーのログオンを拒否したい管理者である場合は、システムパラメータのlocalAuthオプションを無効にする必要があります。

注:

外部サーバーが構成されている必要があります。

コマンドプロンプトで、次のように入力します。

```
set system parameter localAuth <ENABLED|DISABLED>
```

例:

`set system parameter localAuth DISABLED` GUIを使用してこの機能を構成する方法については、「ユーザーアカウントとパスワード管理」を参照してください(/ja-jp/citrix-adc/current-release/system/authentication-and-authorization-for-system-user/user-account-and-password-management.html)。

管理者ユーザーのパスワード変更を強制する: `nsroot` で保護された認証の場合、システムパラメータで `forcePasswordChange` オプションが有効になっていると、NetScalerはユーザーにデフォルトパスワードを新しいパスワードに変更するように促します。デフォルトの資格情報で初めてログインするときに、CLIまたはGUIから `nsroot` パスワードを変更できます。コマンドプロンプトで、次のように入力します。

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

この機能を構成する方法の例については、「ユーザーアカウントとパスワード管理」を参照してください(/ja-jp/citrix-adc/current-release/system/authentication-and-authorization-for-system-user/user-account-and-password-management.html)。

SSHキーとパスワードなしでNetScalerにアクセスする: 多数のNetScalerアプライアンスを管理する必要がある展開では、SSHキーとパスワードなしを使用することを検討してください。この機能を構成する方法については、「SSHキーとパスワードなしでNetScalerアプライアンスにアクセスする」を参照してください(/ja-jp/citrix-hardware-platforms/mpx/netscaler-initial-configuration.html#access-a-citrix-adc-appliance-by-using-ssh-keys-and-no-password)。

データ保護のためのシステムメインキーの作成: Citrix ADC 12.1からCitrix 13.0–71.44では、LDAP認証に必要なサービスアカウントのパスワードや、ローカルに保存されている認証、承認、監査ユーザーアカウントなど、特定のセキュリティパラメータを保護するためにシステムメインキーを作成する必要があります。

注記:

Citrix 13.0ビルド76.31以降では、アップグレードプロセスによってランダムなシステムメインキーがデフォルトで自動的に作成されます。組織のパスワードポリシーに従って、KEKを頻繁に更新してください。

システムメインキーを作成するには:

1. CLIを使用して、システム管理者としてログインします。
2. 次のコマンドを入力します。

```
create kek <passphrase>
```

注記:

- `create kek` コマンドの実行後、KEKはほとんどのパスワード暗号化に使用されます（ローカルユーザーパスワードはKEKで暗号化されません）。
- KEKファイルを削除してはいけません。シェルアクセスがあり、誤ってキーフラグメントファイルを削除した場合、設定の損失、同期の失敗、ログオンの失敗につながる可能性があります。以下に注意してください。
 - ダウングレードする際は、常にインストールされているビルドと一致する古い設定ファイルを使用してください。そうしないと、ログオン、ソース設定、同期、フェイルオーバーが失敗する可能性があります。
 - キーフラグメントファイルのいずれかが失われたり破損したりした場合、機密データの暗号化/復号化が失敗し、その結果、設定の損失、同期の失敗、ログオンの失敗につながる可能性があります。

- パスフレーズは8文字以上である必要があります。

展開済みのNetScalerでキー暗号化キーを更新する:

NetScalerは、展開済みのADCでKEKの更新をサポートしています。KEKを更新するには、次のコマンドを使用します。

```
update kek -level <basic | extended>
```

KEK更新コマンドはNSIPインターフェースでのみサポートされています。このコマンドは次の2つのオプションをサポートしています。

- **基本:** 古いキーをバックアップし、キーを作成して応答します。ファイルの更新が失敗した場合、システムはエラーを報告し、元の状態に戻ります。
- **拡張:** 古いキーをバックアップし、新しいキーを作成します。デフォルトおよび非デフォルトのパーティション下のns.confやns.conf.0などの設定ファイルを更新します。更新中は、すべての設定変更をブロックします。更新が完了すると、NetScalerが応答します。これらのファイル更新のいずれかが失敗した場合、システムはエラーを報告し、元の状態に戻ります。

以前は、NetScalerはノードごとのデフォルトのKEKのみをサポートしていました。KEKを更新するオプションはありませんでした。

セキュリティのベストプラクティスとして、KEKは組織のパスワードポリシーに従って頻繁に変更する必要があります。

アクセス制御リストを使用する:

デフォルトでは、GUIやSSHを含むすべてのプロトコルとポートがNetScalerでアクセス可能です。アクセス制御リスト (ACL) を使用すると、明示的に指定されたユーザーのみがポートとプロトコルにアクセスできるようにすることで、NetScalerを安全に管理できます。

NetScalerへのアクセスを制御するための推奨事項:

- NetScalerへのアクセスをGUIのみに制限するために、NetScaler Gatewayの使用を検討してください。GUI以外のアクセス方法を必要とする管理者向けには、NetScaler Gatewayを、ポート80、443、3010に対してデフォルトの「DENY」ACLで構成する必要がありますが、これらのポートにアクセスするための信頼されたIPアドレスに対しては明示的な「ALLOW」を設定する必要があります。

このポリシーは、以下のNSCLIコマンドを使用して、信頼されたIPアドレスの範囲に拡張できます。

```
add acl local_access allow -srcip 192.168.0.1-192.168.0.3 -destip  
192.168.0.1-192.168.0.3
```

```
apply acIs
```

- SNMPを使用する場合は、ACLでSNMPトラフィックを明示的に許可してください。以下はコマンドの例です:

```
add acl snmp1-ssh ALLOW -srcip 10.0.0.1-10.0.0.20 -destip  
192.168.0.2-192.168.0.3 -destport 161 -protocol udp
```

```
add acl snmp2-ssh ALLOW -srcip 172.16.0.1-172.16.0.20 -destip  
192.168.0.2-192.168.0.3 -destport 161 -protocol udp
```

```
apply acIs
```

上記の例では、クエリが適切に定義されたコミュニティに対するものであっても、このコマンドは定義された2つのサブネットへのすべてのSNMPクエリにアクセスを提供します。

NSIPおよびSNIPアドレスで管理機能を有効にできます。有効にした場合、管理機能へのアクセスを保護するために、ACLを使用してNSIP、SNIPアドレスへのアクセスを提供します。管理者は、pingコマンドでNetScalerにアクセスできないように設定することもできます。

- Open Shortest Path First (OSPF) およびIPSECは、TCPまたはUDPベースのプロトコルではありません。したがって、NetScalerでこれらのプロトコルをサポートする必要がある場合は、ACLを使用してこれらのプロトコルを使用するトラフィックを明示的に許可してください。プロトコル番号でOSPFとIPSECを指定するACLを定義するには、次のコマンドを実行します:

```
add acl allow_ospf allow -protocolnumber 89
```

```
add acl allow_ipsec allow -protocolnumber 50
```

- XML-API Webサービスを使用する場合は、APIインターフェースを保護するために次のタスクを完了してください:
- ACLを使用して、インターフェースにアクセスするためのホストに権限を付与します。たとえば、10.0.0.1-20および172.16.0.1-20のIPアドレス範囲のホストがXML-APIインターフェースにアクセスできるようにするには、次のコマンドを実行します:

```
add acl xml-api1 ALLOW -srcip 10.0.0.1-10.0.0.20 -destip  
192.168.0.2-192.168.0.3 -destport 80 -protocol tcp  
  
add acl xml-api2 ALLOW -srcip 172.16.0.1-172.16.0.20 -destip  
192.168.0.2-192.168.0.3 -destport 80 -protocol tcp  
  
apply acls
```

- 内部ポートにACLを適用するには、次のコマンドを使用します:

```
set l3param -implicitACLAllow DISABLED
```

注記:

implicitACLAllow コマンドのデフォルト値は **ENABLED** です。

- 内部ポートから ACL を削除するには、次のコマンドを使用します。

```
set l3param -implicitACLAllow ENABLED
```

- クライアント側証明書を使用することで、追加のセキュリティを確保できます。クライアント側証明書とクライアント認証の詳細については、[クライアント認証](#) または Knowledge Center の記事 CTX214874: [NetScaler Appliance でファームウェア 10.1 以降のクライアント証明書を作成して使用する](#)方法を参照してください。

管理者ユーザーにロールベースのアクセス制御を使用する:

NetScaler には、オペレーター、読み取り専用、ネットワーク、スーパーユーザーなどの 4 つのコマンドポリシーまたはロールが含まれています。コマンドポリシーを定義し、異なるロールに対して異なる管理アカウントを作成し、そのロールに必要なコマンドポリシーをアカウントに割り当てることもできます。以下は、読み取り専用ユーザーへの読み取り専用アクセスを制限するためのサンプルコマンドのセットです。

```
add system user readonlyuser

bind system user readonlyuser read-only 0
```

ユーザー、ユーザーグループ、またはコマンドポリシーの設定の詳細については、[ユーザー](#)、[ユーザーグループ](#)、および[コマンドポリシー](#) を参照してください。

システムセッションタイムアウトを構成する:

セッションタイムアウト間隔は、使用されていないときにセッション (GUI、CLI、または API) がアクティブなままである期間を制限するために提供されます。NetScaler では、システムセッションタイムアウトを次のレベルで構成できます。

- ユーザーレベルのタイムアウト。特定のユーザーに適用されます。

GUI: **System > User Administration > Users** に移動し、ユーザーを選択して、ユーザーのタイムアウト設定を編集します。CLI: コマンドプロンプトで、次のコマンドを入力します。

```
set system user <name> -timeout <secs>
```

- ユーザーグループレベルのタイムアウト。グループ内のすべてのユーザーに適用されます。

GUI: **System > User Administration > Groups** に移動し、グループを選択して、グループのタイムアウト設定を編集します。CLI: コマンドプロンプトで、次のコマンドを入力します。

```
set system group <groupName> -timeout <secs>
```

- グローバルシステムタイムアウト。すべてのユーザーおよびタイムアウトが構成されていないグループのユーザーに適用されます。

GUI: **System > Settings** に移動し、**Set global system parameters** をクリックして、ANY Client Idle Time-out (secs) パラメーターを設定します。CLI: コマンドプロンプトで、次のコマンドを入力します。

```
set system parameter -timeout <secs>
```

ユーザーに指定されたタイムアウト値が最優先されます。ユーザーにタイムアウトが設定されていない場合、メンバーグループに設定されたタイムアウトが考慮されます。グループにタイムアウトが指定されていない場合（またはユーザーがグループに属していない場合）、グローバルに設定されたタイムアウト値が考慮されます。いずれのレベルでもタイムアウトが設定されていない場合、デフォルト値の900秒がシステムセッションタイムアウトとして設定されます。

セッションタイムアウト値が管理者が設定したタイムアウト値を超えて設定できないように、タイムアウト値を制限することもできます。タイムアウト値は5分から1日の間で制限できます。タイムアウト値を制限するには：

- GUI: **System > Settings** に移動し、**Set global system parameters** をクリックして、Restricted Timeout フィールドを選択します。
- CLI: コマンドプロンプトで、次のコマンドを入力します。

```
set system parameter -restrictedtimeout <ENABLED/DISABLED>
```

ユーザーがrestrictedTimeoutパラメーターを有効にした後、タイムアウト値がすでに1日より大きい値または5分未満の値に設定されている場合、ユーザーはタイムアウト値を変更するように通知されます。ユーザーがタイムアウト値を変更しない場合、デフォルトで、次の再起動時にタイムアウト値は900秒（15分）に再設定されます。

アクセスしている各インターフェースのタイムアウト期間を指定することもできます。ただし、特定のインターフェースに指定されたタイムアウト値は、そのインターフェースにアクセスしているユーザーに設定されたタイムアウト値に制限されます。例えば、ユーザー **publicadmin** のタイムアウト値が20分であるとしします。この場合、インターフェースにアクセスする際、ユーザーは20分以内のタイムアウト値を指定する必要があります。

各インターフェースでタイムアウト期間を設定するには：

- CLI: コマンドプロンプトで、次のコマンドを使用してタイムアウト値を指定します。

```
set cli mode -timeout <secs>
```

- API: ログインペイロードでタイムアウト値を指定します。

ロギングと監視

ネットワークタイムプロトコルを構成する

NetScalerでネットワークタイムプロトコル (NTP) を有効にし、信頼できるネットワークタイムサーバーを使用するように構成することをお勧めします。NTPを有効にすると、ログエントリとシステムイベントに記録される時刻が正確になり、他のネットワークリソースと同期されます。

NTPを構成する際、NTPサーバーが機密パケット内の情報を開示しないように、ntp.confファイルを変更する必要があります。

NetScalerでNTPを構成するには、次のコマンドを実行します。

```
add ntp server <IP_address> 10

enable ntp sync
```

追加する信頼できるNTPサーバーごとにntp.confファイルを変更します。すべてのサーバーエントリに対応するrestrictエントリが必要です。ntp.confファイルは、NetScalerシェルプロンプトから `find . -name ntp.conf` コマンドを実行して見つけることができます。

SNMPを構成する

NetScalerはSNMPプロトコルのバージョン3をサポートしています。SNMPv3には、認証、アクセス制御、データ整合性チェックなどの管理およびセキュリティ機能が組み込まれています。詳細については、「[SNMPv3クエリ用にNetScalerを構成する](#)」を参照してください。

注:

SNMPv1およびSNMPv2の代わりにSNMPv3を使用することをお勧めします。

少なくとも1つのSNMPマネージャーを構成しない場合、NetScalerはネットワーク内のすべてのIPアドレスからのSNMPクエリを受け入れ、応答します。SNMPマネージャーを追加し、この動作を制限するには、次のコマンドを実行します。

```
add snmp manager <IP_address>
```

SNMPが不要な展開では、次のコマンドで機能を無効にする必要があります。

```
set ns ip <IP_Address> -snmp disabled
```

外部NetScalerログホストへのロギングを構成する

NetScaler Audit Serverは、カーネルおよびユーザーレベルのデーモン内のさまざまなモジュールによって収集されたすべての状態およびステータス情報をログに記録します。Audit Serverを使用すると、管理者はイベント履歴を時系列で確認できます。Audit Serverは、NetScalerからログを収集するSYSLOGサーバーに似ています。Audit Serverは、管理者資格情報を使用して1つ以上のNetScalerアプライアンスからログをフェッチします。

- ローカル監査サーバーの構成

NetScalerでローカルの監査サーバーへのログ記録を設定するには、次のコマンドを実行します。

```
> set audit nslogparams -serverip <hostname> -serverport <port>
```

- リモート監査サーバーの設定

リモートコンピューターの監査サーバーにログ記録を設定するには、そのコンピューターに監査サーバーをインストールします。以下は、監査サーバーのオプションの例です。

```
./audserver -help

usage : audserver -[cmds] [cmd arguments]

cmds cmd arguments: -f <filename> -d debug

-help - detail help

-start - cmd arguments, [starts audit server]

-stop - stop audit server

-verify - cmd arguments [verifies config file]

-addns - cmd arguments [add a netscaler to conf file]

-version - prints the version info
```

これらのオプションは、NetScalerのns.logファイルによって生成された監査メッセージのみをログに記録する機能を提供します。すべてのsyslogメッセージをログに記録するには、次の手順を実行します。

1. ローカル機能の/nsconfig/syslog.confファイルからログファイル指定を削除します。
2. ログファイル指定を、リモートsyslogホストのログホスト名またはIPアドレスに置き換えます。次のエントリと同様です。

```
ローカル0.* @10.100.3.53
```

```
ローカル1.* @10.100.3.53
```

3. 前述のログ機能からのログエントリを受け入れるようにsyslogサーバーを設定します。詳細については、syslogサーバーのドキュメントを参照してください。
4. 標準のsyslogソフトウェアを使用するほとんどのUNIXベースのサーバーでは、メッセージとnsvpn.logファイル用のローカル機能構成エントリをsyslog.conf構成ファイルに追加する必要があります。機能の値は、NetScalerで構成された値に対応している必要があります。
5. 任意のUNIXベースのコンピューターのリモートsyslogサーバーは、デフォルトではリモートログをリスンしません。したがって、リモートsyslogサーバーを起動するには、次のコマンドを実行します。

```
syslogd -m 0 -r
```

注:

監査サーバーに展開されているsyslogバリエーションの同等のオプションを参照してください。

セキュアチャネルを介したメッセージのエクスポートを設定する

SSL (Secure Sockets Layer) を介してsyslogを安全にエクスポートすることで、機密性の高いログデータが暗号化され、認証された方法でネットワークを通過することを保証できます。SSLを活用することで、盗聴、改ざん、不正アクセスからsyslogの送信を保護できます。詳細については、[SSLを介してsyslogを安全にエクスポートする](#)を参照してください。

LOM の構成

LOM インターフェイスを保護するために、以下の対策を講じることをお勧めします。

- LOM ポートをインターネットに公開しないでください。
- LOM を SPI ファイアウォールの背後に展開してください。

- LOM を、信頼できないネットワークトラフィックから論理的 (個別の VLAN) または物理的 (個別の LAN) に分離されたネットワークセグメントに展開してください。
- LOM および NetScaler 管理ポートには、異なるユーザー名、パスワード、SSL 証明書、および SSL キーの値を設定してください。
- LOM 管理インターフェイスへのアクセスに使用されるデバイスは、ネットワーク管理専用であり、他の管理デバイスポートと同じ物理 LAN または VLAN にある管理ネットワークセグメントに配置されていることを確認してください。
- LOM IP アドレスを簡単に識別および分離するために、LOM 管理インターフェイスおよび管理サーバー用に特別な IP アドレス (プライベートサブネット) を予約してください。管理対象 NetScaler の LAN インターフェイスで予約済み IP サブネットを使用しないでください。DHCP によって割り当てられた動的 IP アドレスは推奨されません。これは、LAN セグメント外の MAC アドレスに基づいてファイアウォールアクセス制御リストを実装することが困難になるためです。
- パスワードは、英数字と特殊文字を組み合わせた 8 文字以上で設定してください。パスワードは頻繁に変更してください。

アプリケーションとサービス

NetScaler® を構成してアップグレードヘッダーを削除または渡す

バックエンドサーバーへの攻撃を防ぐために、新しいパラメーター `passProtocolUpgrade` が HTTP プロファイルに追加されました。このパラメーターの状態に応じて、アップグレードヘッダーはバックエンドに送信されるリクエストで渡されるか、リクエストを送信する前に削除されます。

- `passProtocolUpgrade` パラメーターが有効になっている場合、アップグレードヘッダーはバックエンドに渡されます。サーバーはアップグレードリクエストを受け入れ、その応答で通知します。
- このパラメーターが無効になっている場合、アップグレードヘッダーは削除され、残りのリクエストはバックエンドに送信されます。

`passProtocolUpgrade` パラメーターは以下のプロファイルに追加されます。

- `nshttp_default_profile` - デフォルトで有効
- `nshttp_default_strict_validation` - デフォルトで無効
- `nshttp_default_internal_apps` - デフォルトで無効
- `nshttp_default_http_quic_profile` - デフォルトで有効

`passProtocolUpgrade` パラメーターを無効に設定することをお勧めします。

CLI を使用して `passProtocolUpgrade` パラメーターを設定する:

コマンドプロンプトで、次のように入力します。

```
set ns httpProfile <name> [-passProtocolUpgrade ( ENABLED | DISABLED )]
```

GUI を使用して `passProtocolUpgrade` パラメーターを設定する:

1. **System -> Profiles -> HTTP Profiles** に移動します。
2. HTTP プロファイルを作成または編集します。
3. **Pass Protocol Upgrade** チェックボックスを選択します。

無効なHTTPリクエストを破棄するようにNetScalerを構成する

無効なHTTPリクエストが仮想サーバーを通過するのを防ぐため、NetScalerを厳密なチェックとHTTPリクエストの適用で構成することをお勧めします。これを行うには、CLIで次のコマンドを使用して、組み込みのHTTPプロファイル `nshttp_default_strict_validation` を1つ以上の仮想サーバーにバインドします。

```
show ns httpProfile (Shows the available http profile (default+user configured profiles))
```

```
set lb vserver <vserver name> -httpProfileName  
nshttp_default_strict_validation
```

このオプションを使用するお客様は、本番環境にリリースする前に、ステージング環境で変更をテストすることをお勧めします。

HTTPデシンク攻撃に対する保護は、厳密なHTTP検証プロファイル

(`nshttp_default_strict_validation`) でデフォルトで有効になっています。クライアントに面するすべてのエンティティに厳密なプロファイルを使用してください。

HTTPリクエスト密輸攻撃とその軽減策の詳細については、サポート記事「[NetScaler - HTTP Request Smuggling Reference Guide](#)」を参照してください。

HTTPサービス拒否攻撃に対する保護を構成する

NetScalerファームウェアは、「スローリード」タイプの攻撃を含むHTTPサービス拒否攻撃に対する限定的な対策をサポートしています。NetScalerシェルプロンプトから `nsapimgr` ユーティリティを使用して、これらの機能を構成できます。

- `small_window_threshold` (デフォルト=1)
- `small_window_idle_timeout` (デフォルト=7秒)
- `small_window_cleanthresh` (デフォルト=100)
- `small_window_protection` (デフォルト=有効)

デフォルト設定は、スローリード攻撃を含むHTTPサービス拒否攻撃を防ぐのに十分ですが、他の攻撃に対してはパラメータの調整が必要になる場合があります。

このような攻撃から保護するには、NetScalerシェルプロンプトから次の `nsapimgr` コマンドを使用して、`small_window_threshold` プロパティを上方調整します。

```
$ nsapimgr -ys small_window_threshold=<desired value>
```

注:

`small_window_threshold` の希望する値は、展開における受信トラフィックパターンに基づいて設定できます。許容範囲は0から2³²です。

NetScalerシェルプロンプトから `nsconmsg -d stats` コマンドを使用して、以下のカウンタを監視することで、HTTPサービス拒否攻撃に対する保護を確認できます。

- `nstcp_cur_zero_win_pcb`: このカウンタは、現在ウィンドウ値が低いPCBの数を追跡します。
- `nstcp_err_conndrop_at_pass`: このカウンタは、NetScalerがパケットを一方から他方へ通過させている間に、`nscfg_small_window_idletimeout` 値を超えたことを検出したときに増加します。
- `nstcp_err_conndrop_at_retx`: このカウンタは、再送信中に経過する時間が `nscfg_small_window_idletimeout` 値を超えたときに増加します。
- `nstcp_cur_pcb`: このカウンタは、KAプローブでプローブされたサージキュー内のPCBの数を追跡します。

このオプションを使用するお客様は、本番環境にリリースする前に、ステージング環境で変更をテストすることをお勧めします。

TCPスプーフィング攻撃から防御するようにNetScalerを構成する

バックエンドサーバーをTCPスプーフィング攻撃から保護するために、次のコマンドを使用できます。

```
set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -spoofSynDrop  
ENABLED
```

Done

```
set lb vserver lbvserver1 -tcpProfileName profile1
```

Done

このオプションを使用するお客様は、本番環境にリリースする前に、ステージング環境で変更をテストすることをお勧めします。

RFC 5961準拠を構成する

NetScalerリリース14.1-4.x以降、TCPプロファイルで `-rfc5961Compliance` オプションが利用可能です。このオプションにはスプーフィング保護が含まれており、`rstWindowAttenuate` と `-spoofSynDrop` の両方をカバーします。各オプションを個別に設定することなく、これらすべての保護を得るには `-rfc5961Compliance` を有効にします。

詳細については、[TCP構成の例](#)を参照してください。

特定のHTTPヘッダーを受け入れるようにNetScalerを構成する

NetScalerを構成して、特定のHTTPヘッダーのみを受け入れるようにすることが可能です。これは、特定の定義済みHTTPヘッダーを持つネットワークトラフィックがバックエンドサーバーに渡されるのを制限するために、書き換えアクションを追加することで実現できます。

次のグローバル書き換えアクションは、Host、Accept、testなどのヘッダーを持つネットワークトラフィックのみをサーバーに送信します。

```
add rewrite action act1 replace_all q/  
HTTP.REQ.FULL_HEADER.after_str("\r\n")/      q{TARGET.REGEX_SELECT(re/  
(iu)^(Host|Accept|test):.*\r\n/) ALT ""} -pattern q{re/(U).+:\r\n/}  
  
add rewrite policy pol1 HTTP.REQ.IS_VALID act1  
  
bind rewrite global pol1 100
```

HTTPヘッダーのヘッダーサイズを構成する

`maxHeaderLen` と `maxHeaderFieldLen` のHTTPヘッダーサイズパラメーターには、ビジネスニーズに適した値を維持することをお勧めします。デフォルト値は24820に設定されており、これは大きなHTTPヘッダーを必要とするアプリケーションとの互換性を保証します。

```
set httpprofile http-prof -maxHeaderLen <header-length> -maxHeaderFieldLen  
<header-field-length>
```

`maxHeaderLen` パラメーターはヘッダー全体のサイズを制御し、`maxHeaderFieldLen` は個々のヘッダーフィールドのサイズを制御します。これらのパラメーターは、バッファオーバーフローやヘッダーインジェクション攻撃などのヘッダーベースの悪用に対する攻撃対象領域を制限することで、セキュリティを強化するために利用できます。ヘッダーサイズは、仮想サーバーに構成されているHTTPプロファイル、およびサービスグループまたは仮想サーバーにバインドされているサービスに設定します。

これらのパラメーターをより低い値に構成することも可能ですが、そうすると、アプリケーションが構成された制限を超えるヘッダーを使用した場合に、正当なリクエストが破棄される可能性があります。したがって、管理者はこれらの値を下げる前に、アプリケーションの要件を慎重に評価する必要があります。

NetScalerでのURLの正規化

URL正規化は、一貫性のないURL形式を単一の予測可能な構造に標準化し、セキュリティルール、検索エンジン、およびWebクローラーが同じWebリソースの異なる表現を同一として扱うようにします。NetScalerは、ネイティブのHTTPプロファイルパラメーターを通じてこれに対処し、攻撃者が正規化されていないURLを悪用してセキュリティフィルターをバイパスするのを防ぐのに役立ちます。

URL正規化は、以下のNetScalerビルドで利用可能です。

- 14.1-73.37以降
- 14.1-73.37 FIPS以降
- 13.1-64.23以降
- 13.1 37.279 FIPS以降

URL正規化パラメータを有効にするには、次のコマンドを使用します。

```
set ns httpProfile <profilename> -normalizeURL ENABLED
```

オリジンサーバーに送信されるリクエストに対してRFC 3986 URL正規化を有効にするには、次のコマンドを使用します。

```
set ns httpProfile <profilename> -normalizeURLtoOrigin ENABLED
```

詳細については、「」([/ja-jp/citrix-adc/current-release/security/normalize-urls.html](https://ja-jp.citrix-adc/current-release/security/normalize-urls.html))を参照してください。

強化されたTCP ISN生成

強化されたISN生成は、NetScalerでのTCP接続設定時（サーバー側のみ）に初期シーケンス番号のランダム性を高め、攻撃者が悪用する可能性のある予測可能性を低減します。このパラメータはデフォルトで無効になっていますが、CLIを使用して有効にできます。

強化されたTCP ISN生成は、以下のNetScalerビルドで利用可能です。

- 14.1-73.37以降
- 14.1-73.37 FIPS以降
- 13.1-64.23以降
- 13.1 37.279 FIPS以降

強化されたISN生成パラメータを有効にするには、次のコマンドを使用します。

```
set ns tcpparam -enhancedISNgeneration ENABLED
```

詳細については、「」([/ja-jp/citrix-adc/current-release/system/tcp-configurations.html#enhanced-isn-generation](https://ja-jp.citrix-adc/current-release/system/tcp-configurations.html#enhanced-isn-generation))を参照してください。

close-notifyの構成

close-notifyは、SSLデータ転送の終了を示すセキュアなメッセージです。RFC 5246に準拠して、クライアントとサーバーは、切断攻撃を回避するために、接続が終了することを知っている必要があります。どちらの当事者も、close_notifyアラートを送信することで、終了メッセージの交換を開始できます。クローズアラートの後に受信したデータは、他の致命的なアラートが送信されていない限り無視されます。各当事者は、接続の書き込み側を閉じる前にclose_notifyアラートを送信する必要があります。TLS終了イベントの監査イベントがキャプチャされるようにするには、スーパーユーザーまたはsysadminとしてCLIにログオンし、次のコマンドを実行します。

```
set ssl parameter -sendCloseNotify y

save ns config
```

管理GUI、NITRO API、およびRPC通信の保護

NetScalerおよびNetScaler Gateway上の管理GUI、NITRO API、およびRPC通信を保護するには、内部HTTP/HTTPSサービスのためにNetScalerで `-maxclient` を設定する必要があります。

```
set service nshttpd-gui-127.0.0.1-80 -maxclient $max_client{}

set service nshttpd-vpn-127.0.0.1-81 -maxclient $max_client{}

set service nshttps-127.0.0.1-443 -maxclient $max_client{}
```

`-maxclient` 値の設定およびこの設定をサポートするNetScalerのバージョンに関する詳細については、[NetScaler GUI](#)、[NetScaler CLI](#)、または[NetScaler NITRO API](#)を使用して内部HTTP GUIサービスを構成するを参照してください。

DNSSEC セキュリティに関する推奨事項

DNSSEC を使用しているお客様には、以下の推奨事項を適用することをお勧めします。

KSK/ZSK 秘密鍵には RSA 1024 ビット以上を使用する

NIST は、DNS 管理者が 01 October 2015 まで 1024 ビットの RSA/SHA-1 または RSA/SHA-256 ZSK を維持することを推奨しています。

DNSSEC キーの有効期限切れに対する SNMP アラームを有効にする

デフォルトでは、NetScaler で DNSSEC キーの有効期限切れに対する SNMP アラームが有効になっています。キーの有効期限切れ通知は、`dnskeyExpiry` と呼ばれる SNMP トラップを介して送信されます。3 つの MIB 変数 `dnskeyName` と `dnskeyUnitsOfExpiry` は、`dnskeyExpiry` SNMP トラップとともに送信されます。詳細については、「NetScaler SNMP OID リファレンス」を参照してください。

x.509 証明書の有効期限が切れる前に KSK/ZSK 秘密鍵をロールオーバーする

NetScaler では、事前公開方式と二重署名方式を使用して、ゾーン署名キーとキー署名キーのロールオーバーを実行できます。詳細については、NetScaler Docs の「[Domain Name System > Configuring DNSSEC](#)」トピックを参照してください。

DNSSEC ADNS サーバーを保護する

NetScaler が DNSSEC プロキシモードで構成されている場合、バックエンド ADNS サーバーからの応答をキャッシュし、キャッシュされた応答を DNS クライアントに転送します。

NetScaler が特定のゾーンの権威サーバーである場合、そのゾーン内のすべてのリソースレコードは NetScaler 上で構成されます。権威ゾーンに署名するには、そのゾーンのキー (ゾーン署名キーとキー署名キー) を作成し、そのキーを NetScaler に追加してから、ゾーンに署名する必要があります。

NetScaler を権威サーバーとして構成するには、次の手順を実行します。

1. ADNS サービスを追加します。

例:

```
add service s1 <ip address> adns 53`
```

2. DNS キーを作成します。

例えば、`com` ドメインの権威サーバーとして機能させるには：

```
create dns key -zoneName com -keytype ksk -algorithm rsASHA512 -keysize  
3000 -fileNamePrefix com.ksk.rsasha1.3000
```

```
create dns key -zoneName com -keytype zsk -algorithm rsASHA512 -keysize  
3000 -fileNamePrefix com.zsk.rsasha1.3000
```

注:

DNSキーは一度作成する必要があり、/nsconfig/dns に保存されます。

3. DNSキーを追加します。

例えば、

```
add dns key com.zsk.3000 /nsconfig/dns/com.zsk.rsasha1.3000.key /  
nsconfig/dns/com.zsk.rsasha1.3000.private
```

```
add dns key com.ksk.3000 /nsconfig/dns/com.ksk.rsasha1.3000.key /  
nsconfig/dns/com.ksk.rsasha1.3000.private
```

4. **com** ゾーンのNSおよびSOAレコードを追加し、その後ゾーンに署名します。

```
add dns soaRec com -originServer n1.com -contact citrix
```

```
add dns nsrec com n1.com
```

```
add dns zone com -proxyMode no
```

```
add dns addRec n1.com 1.1.1.1
```

```
sign dns zone com
```

注: さらに、DNSグローバルパラメーターでDNSEC拡張パラメーターも有効にする必要があります。

NetScalerを権威ドメインネームサーバーとして構成する方法の詳細については、[製品ドキュメント](#)の「ドメインネームシステム > NetScalerをADNSサーバーとして構成する」トピックを参照してください。

レガシー構成

NetScaler®で暗号リダイレクトを無効にするように構成する

暗号リダイレクトを使用すると、SSLハンドシェイクが失敗したときに、正確で意味のあるエラーメッセージを配信するようにSSL仮想サーバーを構成できます。SSLハンドシェイクが失敗すると、NetScalerはユーザーを以前に構成されたURLにリダイレクトします。URLが構成されていない場合、NetScalerは内部で生成されたエラーページを表示します。

コマンドプロンプトで、次のコマンドを実行して暗号リダイレクトを構成し、構成を確認します。

```
set ssl vservice <vServerName> -cipherRedirect DISABLED

show ssl vservice <vServerName>
```

NetScalerでデフォルトのSSLプロファイルを仮想サーバーにバインドすると、その仮想サーバーのSSLパラメーターは、バインドされたプロファイルから継承されます。その結果、SSLプロファイルがこれらの設定を制御するため、仮想サーバーでSSLパラメーターを直接変更することはできません。

```
set ssl profile <ssl Profile name> -cipherRedirect DISABLED
```

詳細については、[暗号リダイレクト](#)を参照してください。

NetScalerでSSL再ネゴシエーション設定を構成する

SSL再ネゴシエーションを無効にすることをお勧めします。

```
set ssl parameter -denySSLReneg ALL
```

プロファイルが有効になっている場合、このパラメーターをフロントエンドプロファイルとバックエンドプロファイルの両方で設定することもお勧めします。

```
set ssl profile <frontend ssl profile name> -denySSLReneg ALL
```

```
set ssl profile <backend ssl profile name> -denySSLReneg ALL
```

詳細については、[-denySSLRenegパラメーターの構成方法と使用方法](#)を参照してください。

NDcPP準拠証明書チェックの設定

NDcPP準拠証明書チェックは、NetScalerがクライアント（バックエンド接続）として機能する場合に適用されます。証明書の検証中に、SSL証明書にSANが存在する場合は、共通名を無視します。

コマンドプロンプトで、次のコマンドを入力してSSLパラメータの「ndcppComplianceCertCheck」属性を設定します。

```
set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB  
<positive_integer>] [-strictCACHecks (YES | NO)] [-sslTriggerTimeout  
<positive_integer>] [-sendCloseNotify (YES | NO)] [-encryptTriggerPktCount  
<positive_integer>] [-denySSLReneg <denySSLReneg>] [-insertionEncoding  
(Unicode|UTF-8)] [-ocspCacheSize <positive_integer>] [- pushFlag  
<positive_integer>] [- dropReqWithNoHostHeader (YES | NO)] [-  
pushEncTriggerTimeout <positive_integer>] [-ndcppComplianceCertCheck ( YES  
| NO)] [-heterogeneousSSLHW (ENABLED | DISABLED )]
```

例:

```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCACHecks no  
-ssltriggerTimeout 100 -sendClosenotify no -encryptTriggerPktCount 45  
-denySSLReneg NONSECURE -insertionEncoding unicode -ocspCacheSize 10  
-pushFlag 3 -dropReqWithNoHostHeader YES -pushEncTriggerTimeout 100 ms  
-ndcppComplianceCertCheck YES
```

NetScaler® 暗号化に関する推奨事項

このセクションでは、NetScaler上で暗号化マテリアルが正しく保護されるようにするために従うべきいくつかの重要な手順を詳しく説明します。また、NetScaler、バックエンドサーバー、およびエンドユーザーを保護するために、このマテリアルを使用するようにNetScalerを構成する方法に関する情報も提供します。

TLS証明書とキーの管理

FIPSおよびNDcPP展開向けTLS暗号スイートの構成

以下のTLS暗号スイートは、FIPSおよびNDcPP展開でサポートされています。

- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1-ECDHE-RSA-AES128-SHA
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-AES256-GCM-SHA384
- TLS1.2-AES128-GCM-SHA256
- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-AES-128-SHA256
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1.2-ECDHE-ECDSA-AES256-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
- TLS1.3-AES256-GCM-SHA384
- TLS1.3-AES128-GCM-SHA256

MPX 14000 FIPSでサポートされている暗号のリストについては、<https://docs.netScaler.com/ja-jp/citrix-adc/downloads/cipher-support-on-netScaler-mpx-sdx-14000-fips.pdf>を参照してください。

NetScalerで承認済みの暗号スイートのみが構成されていることを確認するには、CLIから以下の構成手順を実行します。

1. 仮想サーバーからすべての暗号をアンバインドします。

```
unbind ssl vs v1 -cipherName FIPS
```

2. TLS1-AES-256-CBC-SHA、次にTLS1-AES-128-CBC-SHAのみを次のコマンドでバインドします。

```
bind ssl vs v1 -cipherName <cipher>
```

```
bind ssl vs v1 -cipherName TLS1-AES-256-CBC-SHA
```

信頼されたCAを使用して証明書とキーペアをインストールする:

公開または企業認証局 (CA) から証明書を取得するには、まず秘密鍵と証明書署名要求 (CSR) を生成する必要があります。次の手順を実行します。

1. sysadmin またはスーパーユーザーとして NetScaler CLI に認証します。
2. RSA 秘密鍵を作成します。

```
create fipsKey m1 -keytype RSA -modulus 2048 -exponent F4
```

3. 証明書署名要求 (CSR) を作成します。

```
create certreq csr_1 -fipsKeyName m1 -countryName IN -stateName BA  
-organizationName citrix
```

4. CSR を認証局に提出します。

ほとんどの商用および企業 CA では、CSR は電子メールリクエストで送信されます。ただし、提出方法は企業 CA 環境によって異なる場合があります。CA は有効な証明書を電子メールで返しますが、このアクションも企業 CA によって異なる場合があります。CA から証明書を受け取ったら、安全に /nsconfig/ssl ディレクトリにコピーします。

スーパーユーザーまたはsysadminとしてログインし、CLIから次のコマンドを実行します。 >

```
add ssl certKey ck_1 -cert cert1_1 -fipsKey m1
```

NetScaler -FIPS の推奨事項

FIPSベースの展開におけるNetScaler SDXの構成

既存のFIPSのお客様で、真のマルチテナンシーのためにNetScaler SDXを使用している場合は、TLSを終了し、トラフィックをNetScaler SDXに転送するためにFIPS認定のNetScaler MPXを使用してください。あるいは、Thales外部HSMを使用することも可能です。FIPS暗号カードのパスワードを変更するハードウェアセキュリティモジュール (HSM) を備えたFIPS認定バージョンのNetScalerを使用する場合、デフォルトのセキュリティオフィサー (SO) を変更し、次のように新しいユーザーパスワードを設定します。FIPS対応NetScalerのデフォルトのSOパスワードがわからない場合は、[NetScalerサポート](#)にお問い合わせください。注：このタスクを実行できるのは、スーパーユーザーまたはsysadminのみです。

```
set ssl fips -initHSM Level-2 <soPassword> <oldSoPassword> <user-Password>
[-hsmLabel <string>]

save configuration

initHSM
```

FIPS初期化レベル。NetScalerは現在、レベル2 (FIPS 140-2) をサポートしています。この引数は必須です。可能な値：Level-2

hsmLabel

ハードウェアセキュリティモジュール (HSM) を識別するためのラベル。

最大長：31

注：FIPSカード上のすべてのデータは、上記のコマンドで消去されます。

HSMパスワードを安全な場所に保管する

HSMのパスワードは、会社の運用手順に従って安全な場所に保管する必要があります。

注: HSMは、ログイン試行に3回失敗するとロックされます。ロックされると、動作不能になり、その構成を変更することはできません。

その他の機能

このセクションでは、展開されたアプライアンスのセキュリティを向上させるために、NetScaler Web App Firewall と NetScaler Gateway の両方に適用できる構成変更の例と、複数の階層またはセキュリティを構築するための情報を提供します。このセクションには、NetScaler または NetScaler Gateway を SAML SP または SAML IdP のいずれか、あるいはその両方として使用する場合の構成の詳細に関する情報も含まれています。

詳細については、以下のトピックを参照してください。

- [NetScaler Web App Firewall のセキュリティに関する推奨事項](#)
- [NetScaler Gateway のセキュリティに関する推奨事項](#)

NetScaler® Web App Firewall セキュリティに関する推奨事項

- RFC 準拠チェックの場合、WAF プロファイルのデフォルト `rfcprofile` として 'APFW_RFC_BLOCK' を維持することをお勧めします。
- WAF は `Samesite` クッキー属性値の挿入をサポートしており、クッキーは 'Strict' または 'Lax' の値を選択することで、同一サイトまたはクロスサイトのコンテキストに制限できます。

NetScaler をツーアームモードで展開する

ツーアームモードのインストールでは、NetScaler はユーザーと、NetScaler が保護する Web サーバーの間に物理的に配置されます。接続は NetScaler を通過する必要があります。この配置により、NetScaler を迂回するルートが見つかる可能性が最小限に抑えられます。

'Default Deny' ポリシーを使用する

管理者は、NetScaler Web App Firewall ポリシーに一致しないすべてのリクエストをブロックするために、グローバルレベルで「すべて拒否」ポリシーを使用して NetScaler Web App Firewall を構成することをお勧めします。以下は、グローバルレベルで「すべて拒否」ポリシーを構成するためのコマンドのサンプルセットです。

```
add appfw profile default_deny_profile -defaults advanced

add appfw policy default_deny_policy true default_deny_profile
```

```
bind appfw global default_deny_policy <PRIORITY>
```

注:

PRIORITY 設定は、デフォルトポリシーが最後に評価されるようにする必要があります（リクエストが他の構成済みポリシーと一致しない場合にのみ）。

NetScaler ソフトウェアには、appfw_block などのデフォルトプロファイルが含まれており、これらを構成すると、NetScaler Web App Firewall ポリシーに一致しないリクエストがブロックされます。デフォルトプロファイルを設定するには、次のコマンドを実行します。

```
set appfw settings -defaultProfile appfw_block
```

NetScaler Web App Firewall – 複数のセキュリティ層を構築する

以下のガイドラインは、環境とサポートされているアプリケーションに応じて、複数のセキュリティ層を構築するのに役立ちます。

各層で **sessionCookieName** パラメータに異なる値を設定します。

```
set appfw settings -sessionCookieName "citrix_ns_id_1"
```

セキュリティの第一層

セキュリティの第一層を構築するには、以下を実行します。

- バッファオーバーフロー、SQLインジェクション、クロスサイトスクリプティングを有効にします。
- アプリケーションがアクセスすべきURLを特定し、強制ブラウジングから保護する必要がある場合、開始URLが必要です。
- アプリケーションがフォームフィールドでの入力を期待している場合は、フィールド形式チェックを有効にします。

多くの企業が同一生成元ポリシーに違反するJavaScript強化ウェブコンテンツを大量に導入しているため、クロスサイトスクリプティングチェックは誤検知を生成する可能性があります。そのようなサイトでHTMLクロスサイトスクリプティングチェックを有効にする場合、チェックが正当なアクティビティをブロックしないように、適切な例外を生成する必要があります。

最初の層を展開し、誤検知を探し、例外をデプロイしてから、次の層に進みます。段階的な実装は、AppFwの展開管理に役立ちます。

セキュリティの第2層

セキュリティの第2層を構築するには、以下を実行します。

バッファオーバーフロー、SQLインジェクション、クロスサイトスクリプティングに加えて、プロファイルでシグネチャを有効にします。1300以上のシグネチャがあります。すべてのシグネチャールールを有効にするのではなく、アプリケーションの保護に適用できるシグネチャのみを有効にしてください。

第2層を展開し、誤検知を探し、例外をデプロイしてから、次の層に進みます。段階的な実装は、NetScaler Web App Firewallの展開管理に役立ちます。

セキュリティの第3層

セキュリティの第3層を構築するには、以下を実行します。

- アプリケーションのニーズに基づいて、CSRFタグ付け、Cookieの一貫性、フォームフィールドの一貫性などの高度なプロファイルセキュリティチェックを、それらを必要とするアプリケーションの部分で有効にします。
- 高度なセキュリティチェックはより多くの処理を必要とし、パフォーマンスに影響を与える可能性があります。アプリケーションが高度なセキュリティを必要としない限り、基本的なプロファイルから開始し、アプリケーションの要件に応じてセキュリティを強化することをお勧めします。

基本的なNetScaler Web App Firewallプロファイルで無効になっているセキュリティチェックはすべて、HTTP応答内のオブジェクトに対して動作します。そのため、これらのセキュリティチェックはより多くのリソースを消費します。NetScaler Web App Firewallが応答側の保護を実行する場合、個々のクライアントに送信された情報を記憶する必要があります。たとえば、フォームがNetScaler Web App Firewallによって保護されている場合、応答で送信されたフォームフィールド情報はメモリに保持されます。クライアントが次の後続のリクエストでフォームを送信すると、情報がWebサーバーに送信される前に不整合がないかチェックされます。この概念はセッション化と呼ばれます。開始URL内のURLエンクロージャ、Cookieの一貫性、フォームフィールドの一貫性、CSRFフォームタグ付けなどのセキュリティチェックはすべてセッション化を意味します。これらのセキュリティチェックによって使用されるCPUおよびメモリリソースの量は、NetScaler Web App Firewallを介して送信されるリクエストの数に比例して増加します。例：

- フォームフィールドの一貫性チェックを有効にする：このチェックは、Webフォームがクライアントによって不適切に改変されていないかを確認するために必要です。フォームで重要な情報を提供およびホストするアプリケーションには、このチェックが必要です。

- **CSRFフォームタグ付けチェック:** このチェックはフォーム用です。クロスサイトリクエストフォージェリ (CSRF) フォームタグ付けチェックは、保護されたウェブサイトからユーザーに送信される各ウェブフォームに一意で予測不可能なFormIDをタグ付けし、その後、ユーザーから返されたウェブフォームを調べて、提供されたFormIDが正しいことを確認します。このチェックは、クロスサイトリクエストフォージェリ攻撃から保護します。アプリケーションにウェブベースのフォームがある場合、このチェックを有効にする必要があります。このチェックは、ウェブフォームを詳細に分析する他の特定のセキュリティチェックと比較して、CPU処理能力を比較的ほとんど必要としません。したがって、保護されたウェブサイトまたは NetScaler Web App Firewall 自体のパフォーマンスを著しく低下させることなく、大量の攻撃を処理できます。

NetScaler Web App Firewallのワークフローステップ

NetScaler Web App Firewallのワークフローで次の手順を実行します。

1. セキュリティプロファイルを構成します。
2. 既知のすべての脅威に署名を適用します - ネガティブモデル。
3. このセキュリティプロファイルをアクティブ化する必要がある正しいトラフィックフローを検出できるトラフィックポリシーを構成します。

システムを通過する本番トラフィックの準備ができました。フローの最初のレベルが完了しました。さらに、学習インフラストラクチャを構成します。多くの場合、顧客は本番トラフィックで学習を行いたいと考えているため、署名を適用することでリスクを回避できます。次の手順を実行します。

1. 学習インフラストラクチャを構成します。
2. 保護のために学習したルールを展開します。
3. 稼働開始前に、適用された署名とともに学習データを検証します。

NetScaler® Gateway のセキュリティに関する推奨事項

「デフォルト拒否」ポリシーを使用する

管理者は、グループベースでリソースへのアクセスを選択的に有効にするための承認ポリシーの使用に加えて、グローバルレベルで「すべて拒否」ポリシーを使用して NetScaler Gateway を構成することをお勧めします。

デフォルトでは、defaultAuthorizationAction パラメータは DENY に設定されています。この設定を確認し、各ユーザーに明示的なアクセスを許可してください。設定を確認するには、CLI で

`show vpn parameter` コマンドを使用できます。グローバルレベルですべてのリソースを拒否するようにパラメータを設定するには、CLI から次のコマンドを実行します。

```
set vpn parameter -defaultAuthorizationAction DENY
```

サーバー間で TLS1.2 通信を使用する

NetScaler Gateway と LDAP や Web Interface サーバーなどの他のサービス間のリンクには、TLS1.2 または TLS 1.3 を使用することをお勧めします。このプロトコルの古いバージョンである TLS 1.1、TLS 1.0、および SSLv3 以前の使用は推奨されません。

イントラネットアプリケーションを使用する

Intranet Applications 機能を使用して、NetScaler Gateway プラグインによってインターセプトされ、ゲートウェイに送信されるネットワークを定義します。以下は、インターセプトを定義するためのコマンドのサンプルセットです。

```
add vpn intranetApplication intra1 ANY 10.217.0.0 -netmask 255.255.0.0  
-destPort 1-65535 -interception TRANSPARENT
```

```
bind vpn vserver v1 -intranetapp intra1
```

認証、承認、および監査のセキュリティに関する推奨事項

NetScaler または NetScaler Gateway アプライアンスが SAML SP または SAML IdP、あるいはその両方として構成されている場合は、推奨される構成の詳細について記事 [<https://support.citrix.com/article/CTX316577>](https://support.citrix.com/article/CTX316577) を参照してください。

SAML 認証の詳細については、「[SAML 認証](#)」を参照してください。

SAML 署名なしアサーションの拒否

NetScaler を SAML サービスプロバイダー (SP) として構成する場合は、SAML アクションの **Reject Unsigned Assertions** パラメータが **ON** または **Strict** のいずれかに設定されていることを確認してください。

- **ON** (デフォルト): 署名のないアサーションを拒否します。
- **STRICT**: SAML レスポンスとアサーションの両方が署名されていることを確認します。

推奨事項: **STRICT**を使用します。

注:

- SAML IdPがSAMLアサーションとSAML応答の両方の署名をサポートしている場合は、**STRICT**を使用します。
- 最小許容設定として**ON**を使用します。

SAMLアクションで署名なしアサーションを拒否の値を確認するには、次のコマンドを使用します。

```
show samlaction <SAML Action Name> | grep 'Reject unsigned assertion'
```

署名なしアサーションを拒否: ON

設定例:

```
set samlAction <SAML Action Name> -samlRejectUnsignedAssertion <STRICT | ON>
```

nFactor認証のNetScaler Gatewayログイン情報の暗号化を有効にする

nFactor認証を備えたNetScaler Gatewayアプライアンスは、認証プロセス中にクライアント（ブラウザまたはSSOアプリ）から送信されるログイン要求フィールドを暗号化できます。暗号化されたログイン要求フィールドは、ユーザーの機密データが開示されるのを防ぐための追加のセキュリティ層を提供します。

CLIを使用してログイン暗号化を有効にするには、次のコマンドを実行します。

```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

GUIを使用してログイン暗号化を有効にするには

1. **セキュリティ > AAA – アプリケーショントラフィック**に移動します。
2. 認証設定セクションで、**認証AAA設定の変更**をクリックします。
3. 「**AAAパラメータの設定**」ページで、「**ログイン暗号化**」の「**有効**」をクリックします。

ログイン暗号化の詳細については、[nFactor認証におけるNetScaler Gatewayログイン情報の暗号化](#)を参照してください。

認証、承認、監査VPN仮想サーバーおよびNetScaler Gatewayを保護する

認証、承認、監査VPN仮想サーバーおよびNetScaler Gatewayを保護するために、以下の軽減策を推奨します。

1. NetScaler Gatewayで多要素認証が有効になっており、多要素認証の検証要素がLDAP要素の前にあることを確認します。詳細については、[多要素認証の構成](#)を参照してください。
2. 攻撃の一部はNetScaler GatewayのIPアドレスに対してトリガーされ、FQDNに対してではないようなので、目的のFQDNのみを許可するレスポnderポリシーを作成します。

```
add responder policy IP_Block "HTTP.REQ.HOSTNAME.EQ(\"<enter gateway
FQDN here>\").NOT" DROP

bind vpn vserver <vserver name> -policy IP_Block -priority 100 -type
REQUEST
```

3. IPレピュテーションを有効にします。IPレピュテーションを有効にすると、既知の悪意のあるIPアドレスからの要求を破棄し、攻撃の影響を軽減するのに役立ちます。IPレピュテーションを有効にするには、次のコマンドを実行します。

```
enable feature reputation

add responder policy policy_brute_block_ip
"CLIENT.IP.SRC.IPREP_IS_MALICIOUS" DROP

bind vpn vserver <Gateway_vserver_name> -policy policy_brute_block_ip
-priority 50 -gotoPriorityExpression END -type AAA_REQUEST
```

IPレピュテーションの構成方法の詳細については、[IPレピュテーション](#)を参照してください。

4. NetScalerでreCAPTCHAを有効にします。reCAPTCHAの構成方法については、[nFactor認証のreCAPTCHA構成](#)を参照してください。

スプリットDNS値をREMOTEとして構成する

DNS解決を **REMOTE** として構成することをお勧めします。

以下のいずれかの方法を使用してDNS解決を構成できます。

1. `set vpn parameter splitDns REMOTE`
2. `set vpn sessionAction <action-name> splitDns REMOTE`

`sessionAction` での `splitDns` の構成はオプションです。 `sessionAction` で `splitDns` が提供されない場合、ゲートウェイは `vpn parameter` 構成から `splitDns` 値を取得します。

もし `sessionAction` で `splitDns` が設定されている場合、 `sessionAction` の設定が `vpn parameter` の設定よりも優先されます。

デフォルトでは、CLI は `vpn parameter splitDns` を `BOTH` に設定します。この値を `REMOTE` として設定することをお勧めします。

NetScaler® Consoleセキュリティのベストプラクティス

NetScaler Consoleは、管理者にエンタープライズ全体の可視性を提供し、複数のインスタンスで実行する必要がある管理ジョブを自動化することで、運用を簡素化する一元管理ソリューションです。NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler CPX、NetScaler GatewayなどのNetScaler製品を管理および監視できます。NetScaler Consoleを使用すると、単一の統合コンソールからグローバルなアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングできます。

NetScaler Consoleは、Citrix XenServer、VMware ESXi、Linux KVM上で動作する仮想アプライアンスです。NetScaler Consoleは、Webアプリケーションおよび仮想デスクトップのトラフィックに関する以下の詳細情報を収集することで、アプリケーションの可視性に関する課題に対処します。

- ユーザーセッションレベルの情報
- Webページのパフォーマンスデータ
- サイトのNetScalerインスタンスを介して流れるデータベース情報、および実用的なレポートを提供します。

NetScaler Consoleを使用すると、IT管理者は顧客の問題をわずか数分でトラブルシューティングし、プロアクティブに監視できます。

展開ライフサイクル全体でセキュリティを維持するために、以下の考慮事項を推奨します。

NetScaler Console IPアドレスとNetScalerエージェントIPアドレスをインターネットに公開しないでください

NetScaler Console IPアドレスとNetScalerエージェントIPアドレスをパブリックインターネットに公開せず、適切なステートフルパケットインスペクション (SPI) ファイアウォールの背後に展開することを推奨します。

システムユーザー向けの強力なパスワード

NetScaler Consoleで作成されたシステムユーザーアカウントには、強力なパスワードを使用することを推奨します。パスワードの複雑さの要件の例は次のとおりです。

- パスワードは8文字以上の長さである必要があります。
- パスワードには、辞書に載っている単語や、辞書に載っている単語の組み合わせを含めてはなりません。
- パスワードには、少なくとも1つの大文字、1つの小文字、1つの数字、および1つの特殊文字を含める必要があります。

NetScaler Console を使用して最小パスワード長を設定するには:

1. > に移動します。
2. ページで、右側の をクリックします。
3. を選択します。
4. ページで、最小パスワード長を 8 に指定します。
5. をクリックします。

デフォルトの証明書を変更する

NetScaler Console の初期設定中に、デフォルトの TLS 証明書が作成されます。これらの証明書は、本番環境での展開を意図したものではなく、置き換える必要があります。

NetScaler Console を、信頼できる認証局 (CA) からの証明書、またはエンタープライズ認証局からの適切な証明書を使用するように構成することをお勧めします。詳細については、「[SSL 証明書のインストール](#)」を参照してください。

NetScaler Console に SSL 証明書をインストールするには:

1. > に移動します。
2. で、 をクリックします。
3. ページで、証明書ファイルとキーファイルを選択し、秘密キーが暗号化されている場合はオプションでパスワードを指定します。
4. をクリックします。

ローカル認証を無効にする

NetScaler Consoleで外部認証が構成されており、管理者としてローカルシステムユーザーが管理アクセスにログオンするのを拒否したい場合は、ローカル認証を無効にする必要があります。詳細については、[外部認証を有効にする](#)を参照してください。

注:

外部サーバーを構成する必要があります。

ローカル認証を無効にするには:

1. **設定 > 認証**に移動します。
2. **認証**ページで、**設定**をクリックします。
3. **認証設定**ページで、**サーバータイプ**で「EXTERNAL」を選択します。
4. **挿入**をクリックし、**外部サーバー**ページで、カスケードする認証サーバーを1つまたは複数選択します。
5. ローカル認証を無効にするには、**フォールバックローカル認証を有効にする**のチェックを外します。
6. **OK**をクリックします。

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.