

ネットワークセキュリティ対策によるセキュアなサーバ管理

○原 祐一

名古屋大学 全学技術センター 工学系技術支援室 情報通信技術系技術課

1 はじめに

IT はさまざまな業務において、なくてはならない技術へと進歩し、IT 技術の進歩と同時に個人情報の保護をはじめとする情報セキュリティ対策も情報系の技術者として無視することができない業務となった。このような社会的流れの中でサーバのセキュリティ対策は必須である。しかし、管理するサーバ数が増えれば増えるほど、セキュリティホールが発生しやすくなり、サーバ数に比例してリスクが上昇すると考えられる。そのため、サーバの上位にあたるゲートウェイでのセキュリティ対策を検討した。

2 セキュアなサーバ管理方法概要

今回、サーバの上位にあたるゲートウェイに L3 スイッチとして適応型セキュリティプライアンス機器を導入した。管理しているサーバをすべてプライベート IP アドレスとして、管理方法は VLAN を採用した。また、緊急時のサーバトラブル時に出張などで職場にいないときでも VPN を利用してセキュアなリモート暗号化通信によるサーバトラブル対応ができるようにした。このように、DMZ に近いかたちとして、今までよりもセキュアなネットワークセキュリティ対策によるサーバ管理を行うことができる。

3 サーバ室 ネットワーク構成

3.1 サーバ室 ネットワークイメージ図

- ・ 管理するサーバの上位に L3 スイッチとして、セキュリティプライアンス機器を設置
- ・ セキュリティプライアンス機器のファイアウォール、VLAN、VPN を利用可能とする
- ・ 管理サーバは、プライベート IP アドレス (10.0.0.0/255.0.0.0) を利用して、学外からアクセス可と学内のみアクセス可に分ける

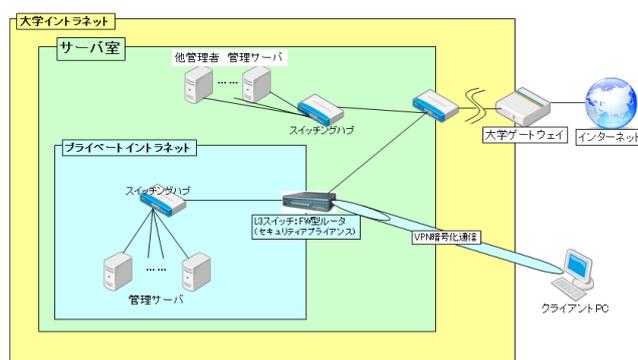


図 1. ネットワークイメージ図

管理サーバ：

DNS サーバ、メールサーバ、アプリケーションサーバ、仮想サーバ (内 Web サーバ)
バックアップサーバ

3.2 設置したセキュリティアプライアンス機器

<p>図 2. ASA5505</p> 	<p>Cisco Systems ASA5505 Security Plus</p> <p>主な仕様</p> <ul style="list-style-type: none"> • 最大 Firewall スループット : 150Mbps • 最大 VPN スループット : 100Mbps • 最大 IPSec VPN ピア数 : 25 • 最大 VLAN 数 : 20
---	---

4 ASA5505 各種設定

基本設定はコンソールで直接機器接続して行い、管理は用意されている GUI 管理ツールで行う。また、ルーテッドモードとファイアウォール透過モードの設定が可能である。今回、プライベートイントラネットを構築するため、ルーテッドモードで構築する。

4.1 VLAN

今回はサーバ管理が主であるため、ポート VLAN を使用する。

ASA5505 Security Plus は、20 個まで VLAN を設定可能である。今回は外部から通信するための VLAN と大学内からのアクセスのみ可、大学外からもアクセスの 3 つの VLAN を作成する。

VLAN100 : 外部通信用

VLAN200 : 学外からアクセス可用

VLAN300 : 学内のみアクセス可用

表 1. ポート VLAN 作成コマンド

VLAN100	VLAN200	VLAN300
<code># interface vlan 100</code>	<code># interface vlan 200</code>	<code># interface vlan 300</code>
<code># security-level 0</code>	<code># security-level 50</code>	<code># security-level 100</code>
<code># nameif outside</code>	<code># nameif open_campus</code>	<code># nameif only_campus</code>
<code># ip address 133.a.b.c 255.255.248.0</code>	<code># ip address 10.1.1.1 255.255.255.0</code>	<code># ip address 10.1.2.1.255.255.255.0</code>
<code># no shutdown</code>	<code># no shutdown</code>	<code># no shutdown</code>

※ VLAN200 と VLAN300 は、セキュリティレベルを変更して、お互いのトラフィックの影響を受けないように設定した。

表 2. 各物理インターフェースに割り当てる VLAN

Eth0/0	Eth0/1	Eth0/2	Eth0/3	Eth0/4	Eth0/5	Eth0/6	Eth0/7
VLAN100	VLAN200	VLAN200	VLAN300	VLAN300	VLAN300	—	—

※ 「Eth0/6」「Eth0/7」は仕様が異なるため割り当てない。

表 3. スイッチに VLAN を割り当てるコマンド

<pre># interface 0/1 # switchport access vlan 100 # no shutdown</pre>

4.2 ASA5505 から外部のネットワークに接続する設定

VLAN100 から外部ネットワークに接続できるようにし、VLAN200 のゲートウェイを VLAN100 のゲートウェイに変換する。

表 4. 外部ネットワーク接続設定

```
# route outside 0.0.0.0 0.0.0.0 133.a.b.254 1
# global (outside) 1 interface
# nat (open_campus) 1 133.a.b.0 255.255.248.0
# static(outside,open_campus) 10.6.1.254 10.6.1.254 network 255.255.255.255
```

※ 「OSPF」「RIP」「EIGRP」によるルーティング設定も可能

4.3 ファイアウォール

- NAT ルールの設定

プライベート IP アドレスとグローバル IP アドレスを関連付ける。関連付けを行わないと利用できないようにすることで、被害はプライベートネットワーク内のみに留めることができることからネットワークの不正利用を防ぐことができる。

表 5. NAT ルール設定

		プライベート IP アドレス	グローバル IP アドレス
VLAN200	サーバ 1	10.1.1.10	133.a.b.c
VLAN200	サーバ 2	10.1.1.11	133.a.b.d
VLAN300	サーバ 3	10.1.2.10	133.a.b.e
VLAN300	サーバ 4	10.1.2.11	133.a.b.f

※ プライベート IP アドレスとグローバル IP アドレスは仮の設定である。

表 6. NAT ルール設定コマンド

```
# static (open_campus,outside) 133.a.b.c 10.1.1.10 netmask 255.255.255.255
# static (open_campus,outside) 133.a.b.d 10.1.1.11 netmask 255.255.255.255
# static (only_campus,outside) 133.a.b.e 10.1.2.10 netmask 255.255.255.255
# static (only_campus,outside) 133.a.b.f 10.1.2.11 netmask 255.255.255.255
```

- IP アドレスをキーとして、ポート単位で利用許可の設定

サーバに到達してからソフトウェアファイアウォールで通信を遮断するよりも、サーバに到達する前のゲートウェイで通信を遮断するため、セキュリティレベルを高めることができる。

表 7. ポートアクセスルール

		Source	Destination	Action	サービス
VLAN200	IN	any	any	Permit	icmp
		10.1.1.10	any	Permit	tcp-udp/53,tcp/80,tcp/443
		any	any	Deny	
	OUT	any	any	Permit	Icmp
		any	133.a.b.c (10.1.1.10)	Permit	Tcp/80,tcp/443
		133.a.0.0/255.255.0.0	133.a.b.c (10.1.1.10)	Permit	Tcp/21,tcp/22,tcp-udp/53
		any	any	Deny	

表 8. ポートアクセスルールコマンド

IN の設定
access-list inside_access_in extended permit object-group DM_INLINE_SERVICE_1 10.6.1.0 255.255.255.0 any
object-group service DM_INLINE_SERVICE_1
service-object icmp
access-list inside_access_in extended permit object-group DM_INLINE_SERVICE_2 10.6.1.10 255.255.255.255 any
object-group service DM_INLINE_SERVICE_2
service object-group service tcp-udp eq domain
service object-group service tcp eq http
service object-group service tcp eq https
OUT の設定
access-list outside_access_in extended permit object-group DN_INLINE_SERVICE_3 icmp any any
access-list outside_access_in extended permit object-group DN_INLINE_SERVICE_3 133.a.0.0 255.255.0.0 host 133.a.b.c
object-group service DM_INLINE_SERVICE_4
service object-group service tcp ftp
service object-group service tcp ssh
service object-group service tcp-udp domains

4.4 管理

Cisco のセキュリティアプライアンス製品は GUI 管理ツールが用意されているので、設定の追加・変更・削除は管理ツールにて行う。(管理ツール : Cisco ASDM)

表 9. ASDM 利用許可コマンド

```
# http server enable
# http 133.a.b.x 255.255.255.255 outside
# http 10.1.2.x 255.255.255.255 only_campus
```

- ※ 「133.a.b.x」 は外部ネットワークから管理を許可するパソコン
- ※ 「10.1.2.x」 は内部ネットワークから管理を許可するパソコン

管理ツールは管理パソコン (クライアント PC 可) 上で起動するタイプである



図 3. 管理ツール

5 遠隔地からのサーバ管理

遠隔地からサーバを操作する場合、ネットワークの盗聴が考えられ、情報漏えいの危険性が高い。特にサーバ管理を行う上でパスワードを盗みとられることは致命的である。セキュリティを確保しつつ、サーバトラブルの緊急時に VPN 通信にて通信経路を暗号化することで、セキュアな環境でサーバ管理を行う。

管理ツール「ASDM」には、VPN 接続を設定するウィザードがあるので、比較的簡単に初期設定をすることができる。

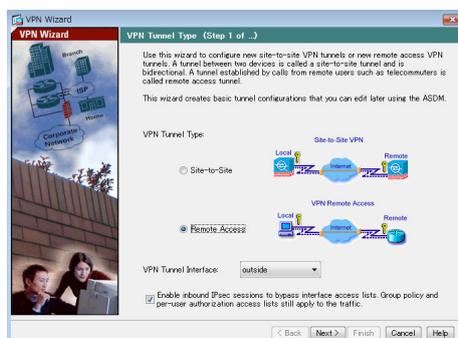


図 4. VPN ウィザード画面

Cisco ASA5505 は、クライアントパソコンから VPN 通信用できるアプリケーション VPN ツール「VPN Client」が用意されている。クライアント PC にインストールすると利用可能となる。今回、パスワードによる認証によって ASA5505 への VPN 接続を許可するように設定をした。今後、よりセキュリティレベルを高めるため、証明書による認証も実現させる予定である。

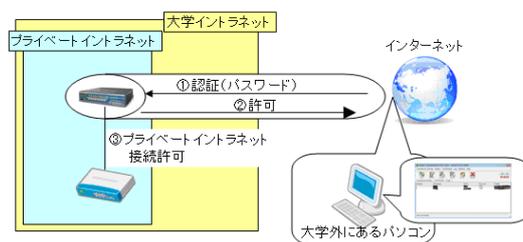


図 5. VPN 接続許可

VPN 接続に成功すると🔒が🔓となり、ASA5505 で許可されたサービスを利用することができる。

6 セキュリティアプライアンス機器導入後

スループット 150Mbps のファイアウォールを仲介するようにしたことで、サーバへの応答スピードが遅くなるのではないかと懸念したが、今までと同じスピードで利用できるのでスループットは問題ないと感じた。また、機器を導入して 6 ヶ月経過したが、機器自体も安定しており、不具合は発生していない。十分運用していくことができると感じた。不正に SSH 接続を試みってくるマシンに対して、サーバに到達前に遮断できているので、導入のメリットはあったと思う。

また、今回想定していないメリットもあった。サーバ室がある建物を建て替えるためサーバ室を移転する必要があり、IP アドレスも変わる事となった。グローバル IP アドレスをすべて ASA5505 で管理していたため、ASA5505 の設定変更のみで、サーバ自体の設定を変更する必要がなかったため、サーバ移転を短時間で行うことができた。

今後の課題

- ・ ASA5505 の不正アクセスも含めたログが一定期間で消えてしまうため、syslog サーバを構築してログを残すようにする必要がある
- ・ ASA5505 は 1 台で運用しているため ASA5505 が故障したとき、影響が大きくなる。機器内部の設定のバックアップ方法を考える必要がある
- ・ もう 1 台機器を購入し、2 台体制のフェイルオーバーを実現して、可用性、安全性を高める必要がある

参考文献

- [1] Cisco WAN 実践ケーススタディ (IP-VPN・広域イーサからハイブリッド VPN・セキュリティ・運用管理まで) 発行) (株) インプレスジャパン