

## DoS/DDoS 対策について（検証）

### 1. はじめに

近年、コンピュータ・ネットワークは社会基盤に浸透し、国民生活において必要不可欠なものとなっていることから、これらが麻痺した場合、国民生活や社会経済活動が重大な被害を受ける可能性がある。ゆえに、コンピュータ・ネットワークの可用性を阻害する DoS/DDoS 攻撃の脅威は現実の問題となっている。

しかしながら、DoS/DDoS 攻撃に対処する防御機能を定量的に調査したものが未だ存在しないと料され、そこで一般的な防御機能について検証を行い有効性の確認を行った。

その結果、攻撃パケットのプロトコル種別、パケット長又は送信元偽装の有無等の特徴に鑑みた最適な防御機能を選択し、正確な設定・運用を行うことにより、一般的に実装されている機能であっても効果が期待できることを確認した。

### 2. 検証結果

#### 2.1 SYNflood攻撃

SYNFlood 攻撃は、TCP のコネクションの成立を行わず、ハーフオープン状態のコネクションを大量に発生させることを企図した攻撃である。また、通常、攻撃パケットの送信元 IP アドレスは偽装され、攻撃元の特特定は困難である。この SYNflood 攻撃に対する防御策の有効性や各機器の挙動などについて検証を行った。

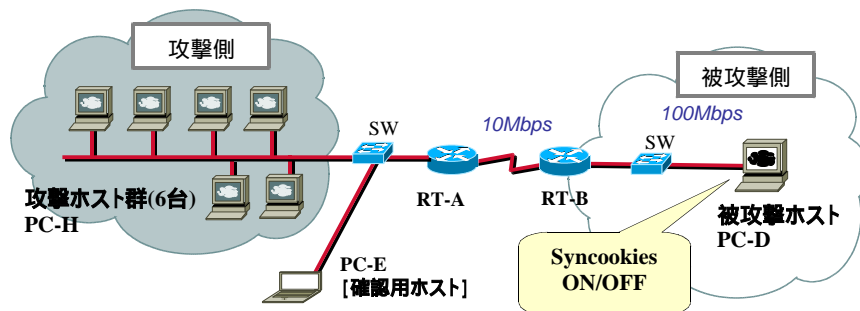


図 2.1 syncookies 機能の有効性検証ネットワーク構成図（別紙 主要機器諸元参照）

#### 2.1.1 syncookies機能の有効性の検証

##### (1) 概要

syncookies<sup>(注 1)</sup>は、TCP コネクションの管理領域がなくても ACK パケットを受理でき、正常な接続要求に対してはコネクションを確立できるようにする機能である。Linux 等で広く実装されている本機能の有効性を確認した。

##### (2) 環境

構成図を図 2.1 に示す。攻撃側は同一仕様・設定のホスト 6 台を利用し、これらに SYNflood 攻撃用ツールをインストールした。被攻撃ホストでは Web サーバを動作させ、その Web サーバの動作状態を確認するために確認用ホストを接続した。

##### (3) 条件

###### (a) 攻撃ホスト [PC-H<sup>(注 2)</sup>]

- ・ 一台あたり 50pps<sup>(注 3)</sup>の SYN パケットを発生するホストを、1 台～6 台それぞれについて検証を実施した。  
( 50,100,150,200,250,300pps )
- ・ 攻撃ツールは、インターネット上で広く流布されている SYNflood 攻撃用ツールを利用した。このツールは送信元アドレスをランダムな値に偽装し、任意の宛先アドレス、宛先ポートに対して SYN パケット ( 64byte ) を 50pps で送信することができる。

(b) 被攻撃ホスト [PC-D<sup>(注 2)</sup>]

- ・ iptables を無効<sup>(注 4)</sup>にしてある他はデフォルト設定とした。
- ・ Web サーバは Apache1.3.28 を使用。設定はデフォルトを使用した。
- ・ syncookies の設定は以下のとおり。

【有効】 sysctl -w "net.ipv4.tcp\_syncookies=1"

【無効】 sysctl -w "net.ipv4.tcp\_syncookies=0"

(c) 確認用ホスト [PC-E<sup>(注 2)</sup>]

確認用ホストでインターネットエクスプローラを利用し、閲覧の可否及びページ表示の待ち時間を測定した。なお、タイムアウトの設定は 15 秒とした。

(4) 方法

被攻撃ホストに syncookies 機能の設定（有効/無効）を行い、SYNFlood 攻撃を実施。その際に Web 閲覧状況の確認及び、リソース消費状態の確認を行った。なお、Web 閲覧状況の確認は 20 回のリクエストを要求し、その応答時間の平均値を算出した。

(5) 結果

図 2.2 のとおり、syncookies 機能無効時の場合は SYNFlood 攻撃が 100pps 程度の攻撃であるにも関わらず、Web 閲覧のタイムアウトが発生し、150pps ではほとんど閲覧が不可能となった。しかし、同機能を有効にした場合は、150pps においてもタイムアウトは発生せず、応答時間も平常時と変わらない状態であった。また、同時に同機能を設定することによる OS のリソースへの影響を調査したが、同機能の有効/無効に関わらず CPU 使用率は 1% 未満で安定しており、メモリ使用領域も多少の変化はあったものの顕著な影響は確認できなかった。

なお、攻撃負荷が約 200pps 以上になると、被攻撃ホストにおいて図 2.3 のようなシステムログ (syslog) が出力された。これは、SYNFlood 攻撃の影響を受けていることを示唆している。

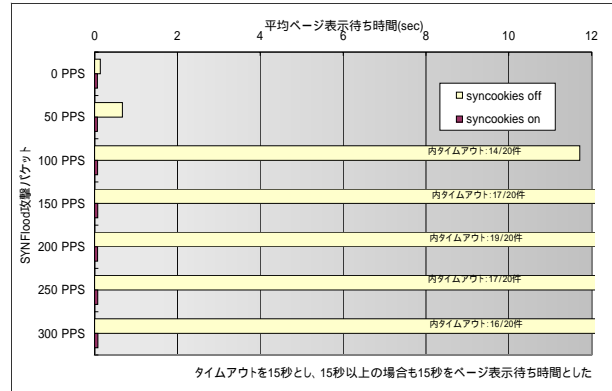


図 2.2 syncookies 有効性検証結果

【syncookies 無効時】

Oct 8 14:41:30 ML350SA304 kernel: NET: 864 messages suppressed.

Oct 8 14:41:36 ML350SA304 kernel: NET: 125 messages suppressed.

Oct 8 14:41:45 ML350SA304 kernel: NET: 99 messages suppressed.

【syncookies 有効時】

Oct 8 14:44:12 ML350SA304 kernel: possible SYN flooding on port 80. Sending cookies.

図 2.3 SYNFlood 攻撃を受けた機器が出力したシステムログ

(6) 考察

SYNFlood 攻撃の状況下において、syncookies 機能は有効に作用することが分かる。なお、本機能は TCP を利用する上位の全プロトコルに影響を与えるため、OS やアプリケーションのネットワーク関連パラメータに注意する必要がある。

(7) 付記事項

実際に SYNFlood 攻撃を受けていないにも関わらず、システムログに SYNFlood の警告が出力される場合は、正当なコネクションが過負荷状態に陥っている可能性がある。このような場合は、syncookies 機能 (tcp\_syncookies) を有効にするのではなく、

tcp\_max\_syn\_backlog<sup>(注 5)</sup>

tcp\_synack\_retries<sup>(注 6)</sup>

tcp\_abort\_on\_overflow<sup>(注 7)</sup>

等の値を調整する必要がある。

## 2.1.2 ファイアウォールのSYNFlood防御機能について有効性の検証

### (1) 概要

ファイアウォールには、SYNFlood 攻撃の防御機能を実装しているものが多い。SYNFlood 攻撃の状況下における、ファイアウォールの SYNFlood 防御機能の有効性を確認した。

### (2) 環境

構成図を図 2.4 に示す。2.1.1(2)環境の被攻撃側にファイアウォールを設置した。

### (3) 条件

#### (a) 攻撃ホスト [PC-H]

2.1.1(3)(a)と同様の条件とした。

#### (b) 被攻撃側ファイアウォール [FW<sup>(注 2)</sup>]

- 外部から被攻撃側サーバ宛の 80/TCP を許可し、これ以外の通信は拒否するルールとした。
- SYN Flood Protection 機能<sup>(注 8)</sup>の有効時の閾値は 1pps とした。

#### (c) 被攻撃ホスト [PC-D]

2.1.1(b)と同様の条件で、syncookies 機能は無効とした。

#### (d) 確認用ホスト [PC-E]

2.1.1(c)と同様の条件とした。

### (4) 方法

被攻撃側のファイアウォールに SYNFlood 攻撃の防御機能の設定 (有効/無効)をおこない、被攻撃ホストに対して SYNFlood 攻撃を実施。その時の接続状況、Web 閲覧状況を確認した。

### (5) 結果

結果を図 2.5 に示す。SYNFlood Protection 機能無効の場合、SYNFlood 攻撃が 100pps 程度で Web 閲覧のタイムアウトが発生し、200pps ではほとんど閲覧

が不可能であった。同機能を有効にした場合は、200pps においてもタイムアウトは発生せず、応答時間も平常時と変わらない状態であった。但し、同機能が有効であり、攻撃パケットが 0pps,50pps の時には逆にスループットが下がる結果となった。なお、ファイアウォールにおける CPU 使用率は、本機能の有効又は無効に関わらず、1%程度であった。

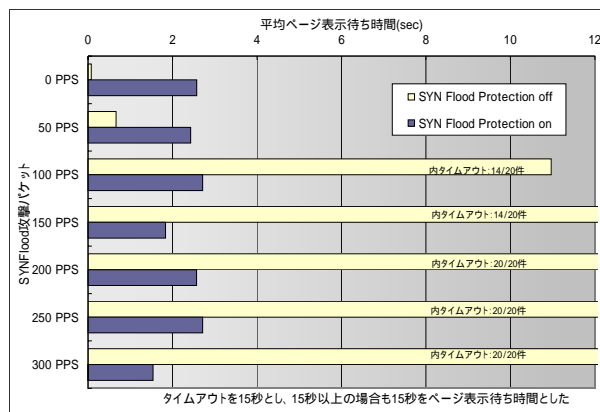


図 2.5 ファイアウォールの SYNFlood 防御機能の効果

### (6) 考察

SYNFlood Protection 機能は、SYNFlood 攻撃に対する防御効果はあるが、常に動作させると、攻撃パケットが少数の場合にはスループットが落ちる。今回の環境でいえば、100pps 程度から本機能が動作することが望ましい。

このような動作は、閾値を設定し、動作を切り替えることにより実現することができるものであり、その閾値を導き出すにはファイアウォールの内側に設置されているサーバの限界値を予め調査することが重要となる。

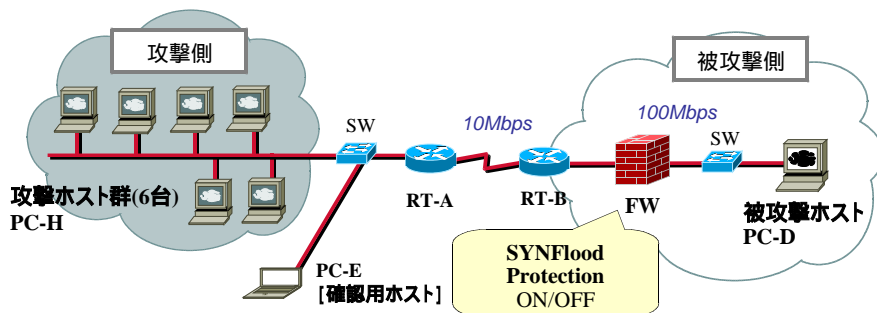


図 2.4 ファイアウォールの SYNFlood 防御機能の有効性検証環境構成図 (別紙 主要機器諸元参照)

### 2.1.3 ルータにおけるQoS機能の効果の検証

#### (1) 概要

SYNFlood 攻撃の状況下において、被攻撃サイトで他の通信の保証を得る為に、ルータの QoS 機能の CAR(Committed Access Rate) 技術<sup>(注<sup>9</sup>)</sup>を利用して、SYN パケットのトラフィック量の制御をおこなう。その際の、サイト内のネットワーク機器への影響を確認した。

#### (2) 環境

構成図を図 2.6 に示す。被攻撃側では、ファイアウォール及び Web サーバを設置。攻撃ホストは FlameThrower<sup>(注<sup>10</sup>)</sup>を利用した。

#### (3) 条件

##### (a) 攻撃ホスト [FlameThrower]

SYNFlood 攻撃パターンを実施、攻撃負荷は 50000pps とした。

##### (b) ルータ [RT-B<sup>(注<sup>2</sup>)</sup>]

- ・ WAN 側インターフェース (Interface A) の input に対して設定した。
- ・ トラフィック量を 2Mbps に制限。なお、設定方法は以下のとおり。

```
Router(config-if)# rate-limit input access-group 100
20000 10000 10000 conform-action
transmit exceed-action drop
```

```
Router(config)# access-list 100 permit tcp any any SYN
```

- ・ 拡張バースト機能は使用せず、適合バーストサイズ及び拡張バーストサイズを同一の値とした。

##### (c) 被攻撃ホスト [PC-D]

- ・ iptables を無効にしてある他はデフォルト設定とした。
- ・ Web サーバは Apache1.3.28 を使用。設定はデフォルトを使用した。

#### (4) 方法

被攻撃側のルータに CAR の設定 (rate

limit の有効/無効) を行い、被攻撃ホストに対して SYNflood 攻撃を実施。その時の通信量、各機器のリソース使用状況を確認した。

#### (5) 結果

表 2.1、表 2.2 に示すとおり、CAR の設定が無効の場合、ファイアウォールでは 8.2Mbps のパケット受信に CPU 使用率は 35%であったが、CAR の設定を有効にすることにより、ルータで若干の CPU リソース消費の増加が認められたものの、ファイアウォールの CPU 使用率は 8%と大きく減少した。

表 2.1 CAR による効果(通信量の比較)

区間	RT-A ~ RT-B	RT-B ~ F/W	F/W ~ Web
CAR無効	8.3 Mbps	8.2 Mbps	6 Mbps
CAR有効	8.3 Mbps	2.4 Mbps	2.3 Mbps

表 2.2 CAR による効果(CPU 使用率の比較)

機器	ルータ	F/W
CAR無効	10%	35%
CAR有効	11%	8%

#### (6) 考察

CAR 機能を利用して、SYNFlood 攻撃のパケットをシステムが許容できる帯域まで下げることにより、自サイト内の機器への影響を抑えることや、他のサービスのための帯域確保ができる。

しかし、正常な通信であるか攻撃パケットを含む異常な通信であるか区別なく帯域制御を行ってしまう。

よって、本機能を利用する場合は、平常時に SYN パケットの通信量を測定し、その値より、若干大きな値を limit として設定することが望ましい。

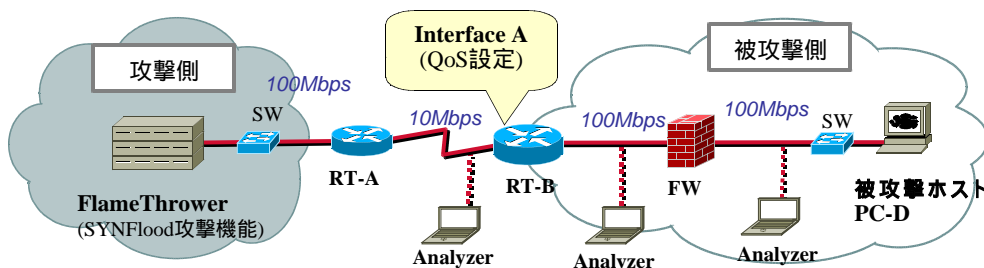


図 2.6 ルータ QoS の有効性検証環境構成図(別紙 主要機器諸元参照)

## 2.2 Connection Flood

Connection Flood 攻撃は、長い時間オープン状態を続けるコネクションを大量に作ることによって、サーバのソケットを占拠することを企図した攻撃である。この Connection Flood 攻撃に対する防御策の有効性や機器の挙動を確認した。

### 2.2.1 TCPコネクションキューの設定値による影響の検証

#### (1) 概要

OS やサーバの TCP コネクションキューに関する設定値を変更した場合における、同時接続数の上限について調査を実施した。なお、TCP コネクションキューに関する設定項目は、以下のとおり。

- ・ Web サーバ最大クライアント数
- ・ TCP コネクションキューのサイズ(以下、「バックログ」という)
- ・ TCP ハンドシェイク完了待ちのコネクションキューの最大サイズ(以下、「ハーフオープンキュー」という)
- ・ TCP ハンドシェイク完了済みのコネクションキューの最大サイズ(以下、「エスタブリッシュキュー」という)

#### (2) 環境

構成図を図 2.7 に示す。2 台の攻撃ホストに Connection Flood 攻撃用ツールをインストールし、被攻撃ホストでは Solaris9 上で Web サーバを起動した。

#### (3) 条件

##### (a) 攻撃ホスト[PC-C<sup>(注 2)</sup>]

インターネット上で広く流布されているツールを利用した。このツールは任意のホスト、TCP ポート及びセッション数の接続を要求し、待ち状態に遷移した後、メソッドを発行せずに任意の時間経過後クローズするもの。

##### (b) 被攻撃ホスト[PC-F<sup>(注 2)</sup>]

- ・ Web サーバは、Apache1.3.28 を使用。
- ・ 最大クライアント数  
MaxClients : 150
- ・ バックログ  
ListenBacklog : 200,400,511(デフォルト),600,800 について実施。
- ・ ハーフオープンキュー  
tcp\_conn\_req\_max\_q0 : 1024(デフォルト)
- ・ エスタブリッシュキュー  
tcp\_conn\_req\_max\_q : 128(デフォルト),200,400,600,800,1000,1200 について実施。なお、設定方法は以下のとおり。

【確認】# ndd -get /dev/tcp tcp\_conn\_req\_max\_q

【設定】# ndd -set /dev/tcp tcp\_conn\_req\_max\_q [value]

#### (4) 方法

被攻撃ホストにおいて、バックログ及びエスタブリッシュキューの設定値を段階的に増加した。その際に、被攻撃ホストから 80/tcp に対して Connection Flood 攻撃を実施。被攻撃ホストにおいて netstat コマンドで同時接続数を確認した。

#### (5) 結果

表 2.3 のとおり、キューに関する設定値を大きくすることにより、より多くの同時接続数を確保することができた。

表 2.3 キューの設定値に対する最大接続数

バックログ エスタブリッシュキュー	200	400	511 (デフォルト)	600	800
128(デフォルト)	278	278	278	278	278
200	350	350	350	350	350
400	451	550	550	550	550
600	451	750	750	750	750
800	451	751	917	950	950
1000	451	751	917	1051	1150
1200	451	751	917	1051	1350

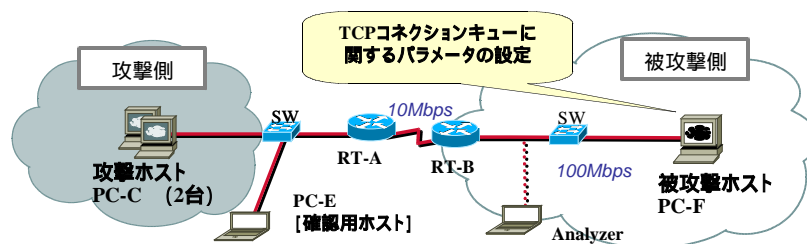


図 2.7 コネクションキュー設定値の影響の検証環境ネットワーク概要図 (別紙 主要機器諸元参照)

しかし、必ずしもバックログ及びエスタブリッシュキューの設定値の増加に応じた、最大同時接続数を確保できるものではなかった。これは、閾値による影響が出ているものであり、" $Tcp\_conn\_req\_max\_q + MaxClients$ " の値と、" $Listenbacklog \times 3/2 + 1 + MaxClients$ " の値を比較し、低い方が適用されるものであると史料される。

実際、表 2.3 中の網掛け部分は前者の計算式、それ以外は後者の計算式の値と合致する。なお、これらキューの動作に関する概念図を図 2.8 に示す。

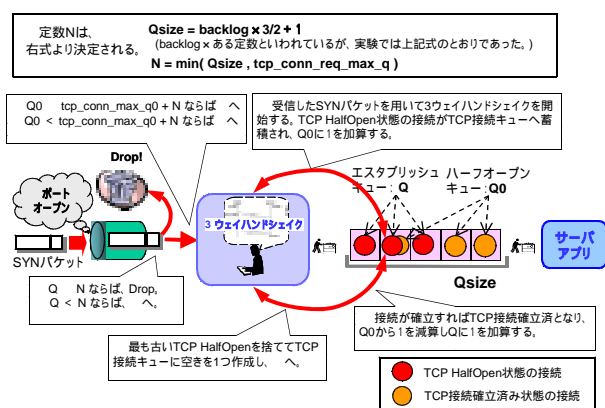


図 2.8 TCP キュー動作概念図 (Solaris9)

## (6) 考察

TCP コネクションキューの値を増やすことにより、より多くの同時接続処理を行うことができる。但し、同値の設定にあたっては、関連するキューの設定を厳密に計算することや、対応するアプリケーションの設定値とあわせた調整を行うことが重要となる。また、最適値を設定するには、サーバが搭載しているメモリなどリソースの状態を考慮するべきである。

Connection Flood 攻撃の防御を行う上

では本機能のみでは不十分であり、他の防御機能と組み合わせた方策をとることが望まれる。

## 2.2.2 ファイアウォールの同時接続数の制限機能による防御の検証

### (1) 概要

Connection Flood 攻撃の状況下において、ファイアウォールの同時接続数制限機能の効果を確認した。

### (2) 環境

構成図を図 2.9 に示す。2.2.1(1)環境の被攻撃側にファイアウォールを設置した。

### (3) 条件

#### (a) 攻撃ホスト [PC-C]

2.2.1(3)(a)と同様の条件とした。

#### (b) 被攻撃側ホスト [PC-F]

- Web サーバは、Apache1.3.28 を使用した。
- 他の設定はデフォルトとした。

#### (c) 被攻撃側ファイアウォール [FW]

- 外部から被攻撃側ホスト宛の 80/TCP を許可し、これ以外の通信は拒否するルールを設定した。
- 同時接続数は、Limit session 機能を利用し、閾値は 30 セッションとした。

SourceIP based threshold : 30

(同一送信元アドレスあたり 30 セッション以上の同時接続を制限)

### (4) 方法

被攻撃側ファイアウォールにおいて同時接続数に関する設定 (有効/無効) を行った上で、被攻撃ホストに対して Connection Flood 攻撃を実施。その際の同時接続数は、被攻撃ホスト上で netstat コマンドにより確認した。

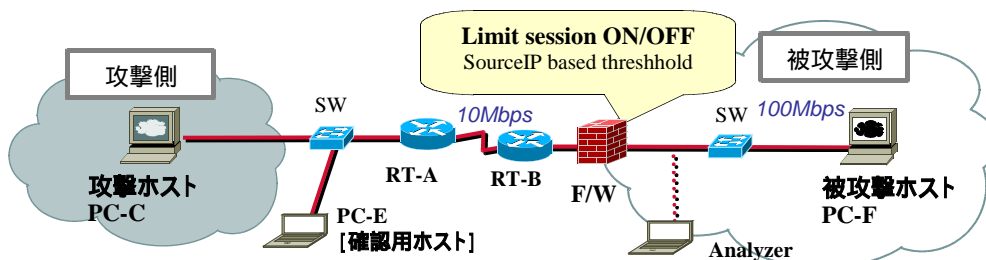


図 2.9 同時接続数の制限機能に関する検証ネットワーク概要図 (別紙 主要機器諸元参照)

## (5) 結果

Connection Flood 攻撃下における、被攻撃ホストの TCP 接続数状態表示結果の出力を図 2.10 に示す。Limit session 機能の無効時は、Web サーバの全接続可能コネクション (278 セッション) を攻撃用ツールにより保持されている。一方、同機能の有効時には設定した閾値 (30 セッション) 以上の接続は制限される。この状態で、他の送信元アドレスからの接続は正常に行うことができた。なお、本機能の有効又は無効に関わらず、ファイアウォールのリソース消費は 1% であった。

```
【limit session 機能無効時】
# netstat -an | awk '{if($1~/80S/ && $7=="ESTABLISHED") print}'
172.16.5.60.80 172.16.1.54.33071 5840 0 49232 0 ESTABLISHED
172.16.5.60.80 172.16.1.54.33072 5840 0 49232 0 ESTABLISHED
.
.
172.16.5.60.80 172.16.1.54.33079 5840 0 49232 0 ESTABLISHED
172.16.5.60.80 172.16.1.54.33080 5840 0 49232 0 ESTABLISHED
# netstat -an | awk '{if($1~/80S/ && $7=="ESTABLISHED") print}' | wc -l
278

【limit session 機能有効時】
# netstat -an | awk '{if($1~/80S/ && $7=="ESTABLISHED") print}'
172.16.5.60.80 172.16.1.54.33071 5840 0 49232 0 ESTABLISHED
172.16.5.60.80 172.16.1.54.33072 5840 0 49232 0 ESTABLISHED
.
.
172.16.5.60.80 172.16.1.54.33079 5840 0 49232 0 ESTABLISHED
172.16.5.60.80 172.16.1.54.33080 5840 0 49232 0 ESTABLISHED
# netstat -an | awk '{if($1~/80S/ && $7=="ESTABLISHED") print}' | wc -l
29
```

図 2.10 同時接続数の確認結果

## (6) 考察

Connection Flood 攻撃は、実際に TCP 3way hand shake を行わないと攻撃が成立しないため、送信元アドレスを偽装することが非常に困難である。よって、送信元アドレス毎の同時接続数を制限する手法は有効に機能する。また、静的な手法ではあるが、送信元アドレスを基にルータやファイアウォールでアクセス制御を行うことも有効である。

## 2.3 UDPFlood

コネクションレス型の通信を行う UDP を利用する UDPFlood 攻撃は、発信元アドレスを偽装される場合が多いため、アクセスリストなどの発信元 IP アドレスによる制限ができない。また、簡単にネットワーク帯域を埋め尽くすことが可能である。この攻撃による、各機器への影響と防御策の有効性について確認した。

### 2.3.1 攻撃パケットサイズの違いによる機器への影響に関する検証

#### (1) 概要

データ部の長さが短いパケット (以下、「ショートパケット」という) と長いパケット (以下、「ロングパケット」という) の 2 種類のパケットを利用して UDPFlood 攻撃を実施した際に、被攻撃側における各機器のリソース (CPU) 状態を確認した。

#### (2) 環境

試験概要を図 2.11 に示す。UDPFlood 攻撃用に、BitStressor<sup>(注 11)</sup> を設置。被攻撃側の構成は、ルータ (RT-B)、ファイアウォール、DNS サーバである。また、各機器間にはネットワークアナライザを設置した。

#### (3) 条件

##### (a) 攻撃側 [BitStressor]

- ・ 攻撃パケットに 2 種類の UDP パケットを準備した。
  - ショートパケット : 64byte
  - ロングパケット : 1500byte
- ・ UDP パケットは DNS クエリーであり、送信元 IP を偽装した。

##### (b) 被攻撃側ルータ [RT-B]

帯域制御やアクセス制御は未設定とした。

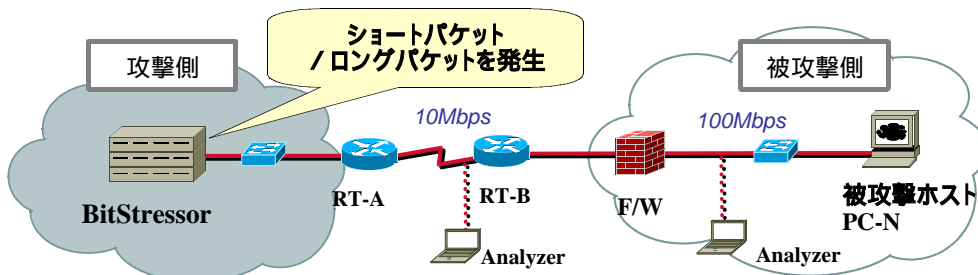


図 2.11 UDPFlood 攻撃試験環境構成図 (別紙 主要機器諸元参照)

(c) 被攻撃側ファイアウォール[FW]  
外部から被攻撃側ホスト宛の 53/  
UDP を許可し、これ以外の通信は拒否  
するルールを設定とした。

(d) 被攻撃側ホスト[PC-N<sup>(注 2)</sup>]  
・ iptables を無効にしてある他はデフ  
ォルト設定とした。  
・ DNS サーバは bind-9.2.1 を利用した。

(4) 方法

BitStressor から予め作成した 2 種類の  
UDP パケットを段階的（平常時～  
10Mbps）に被攻撃側ホストに送信した。  
その時のネットワーク機器におけるリソー  
ス消費状態について測定した。

(5) 結果

図 2.12 に示すとおり、同じ通信量の場合、  
ショートパケットの方が通信量あたりの  
パケット数が多いため、ファイアウォール  
に CPU リソースの消費が顕著に現れ  
た。

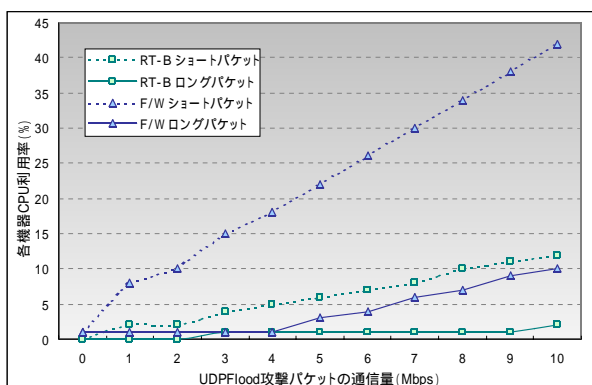


図 2.12 UDPFlood 攻撃時の各機器リソース状態（CPU 使用率）

(6) 考察

通常、WAN 回線は内部回線より帯域  
幅が狭いため UDPFlood 攻撃を受けた場  
合、WAN 回線が輻輳することでシステ  
ム全体の通信に影響を与えることとなる。

ショートパケットの場合は、これに加え  
ネットワーク機器に相当の負担が掛かる。  
防御対策として帯域幅を検討する場合は、  
単位時間あたりの処理バイト数だけでなく  
処理パケット数も考慮することが必要であ  
る。

2.3.2 ネットワークデバイスによる防御対策の  
有効性の検証

(1) 概要

UDPFlood 攻撃の防御策としては帯域  
制御などが一般的対処となるが、攻撃パケ  
ット内容に応じた防御方法が有効である  
と思料されたため、ロングパケット及びシ  
ョートパケットの攻撃に対する防御策につ  
いて、一例を取り上げ検証した。

(2) 環境

2.3.1(2)と同様の環境で実施。

(3) 条件

(a) 攻撃側[BitStressor]

・ 攻撃パケットに 2 種類の UDP パケ  
ットを準備。

ショートパケット：64byte

ロングパケット：1500byte

・ UDP パケットは DNS クエリーで送  
信元 IP を偽装した。

・ 攻撃パケットの通信量は、両パケット  
共に 10Mbps とした。

(b) 被攻撃側ファイアウォール[FW]

2.3.1(3)(c)と同様の条件とした。

(c) 被攻撃側ホスト[PC-N]

2.3.1(3)(d)と同様の条件とした。

(4) 方法

ロングパケットの攻撃に対する防御策と  
してルータによる帯域制御、ショートパケ  
ットの攻撃に対する防御策としてファイ  
アウォールによる帯域制御の有効性につ  
いて確認した。

(5) 結果

(a) ロングパケット対策 - ルータにお  
ける帯域制御

ロングパケット対策として、ルータに  
おいて CAR 機能による帯域制御につ  
いて検証した。

10Mbps のインターフェースに、1M  
bps の帯域制限を実施した。なお、コ  
マンドは以下のとおり。

```
Router(config-if)# rate-limit input access-group 102 1000000
2000 2000 conform-action transmit exceed-action drop
Router(config)# access-list 102 permit udp any any eq 53
```

その結果、ルータ[RT-B]の CPU 使  
用率は 1%から 2%への変化に留まり、

問題なく帯域を制限することが可能であった。

(b) ショートパケット対策 - ファイアウォールによる帯域制御

ショートパケット対策として、転送パケット数の制限について検証した。ファイアウォールの UDPFlood 拒否機能<sup>(注<sup>12)</sup>)</sup>を有効 (Threshold : 1000pps) にし、ショートパケットによる UDPFlood 攻撃を実施した際、ファイアウォール - 被攻撃ホスト間における、通信状況を測定した。その結果を図 2.13 に示す。

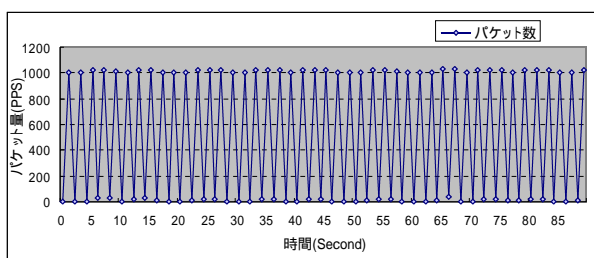


図 2.13 ファイアウォールの UDPFlood 攻撃拒否機能による通信状況

同機器では、閾値で設定した値以上のパケットを受信すると 1 秒間ドロップするため波形のグラフが得られ、結果として帯域制御ができていることが分かる。

(6) 考察

UDP Flood 攻撃は、コネクションレス型の通信を行う UDP を利用しているため、回線の帯域を簡単に圧迫させることができ、ファイアウォールに負荷をかけることもできる。加えて、送信元を偽装するのが容易であり、対策が取りづらい攻撃である。

攻撃パケットが使用しているプロトコル、パケット長及びパケット量や被攻撃側におけるネットワーク機器の処理バイト数、処理パケット数を考慮して、その状態に応じた最適な防御手法をとる必要がある。

ISP などと連携し、より上位のポイントでトラフィックを制御することが望ましい。

2.4 DRDoS 攻撃

DRDoS 攻撃 ( Distributed Reflection Denial of Service の略。) は Reflector と呼ばれる踏み台に送信元を偽装した SYN パケットを送出することで、そこから偽装された送信元に SYN/ACK パケットが発せられる。この仕組みを利用し攻撃先に負荷をかける DDoS 攻撃である。本攻撃が行われた時の機器への影響及び対策について検証を行った。

2.4.1 DRDoS の脅威について検証

(1) 概要

DRDoS 攻撃の状況下において、被攻撃サイトにおけるパケットの発生量について検証を行った。

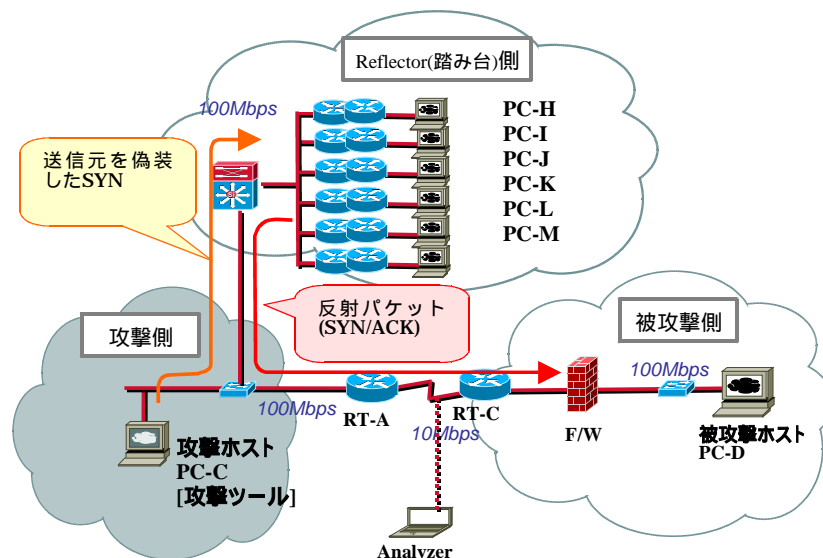


図 2.14 DRDoS 脅威検証環境構成図( 別紙 主要機器諸元参照)

(2) 環境

構成図を図 2.14 に示す。Reflector (踏み台) サイト、攻撃サイト及び被攻撃サイトの 3 サイトを想定し、Reflector (踏み台) サイトには、Reflector に利用する多数のホストを設置した。

(3) 条件

(a) 攻撃ホスト [PC-C]

- ・インターネット上で広く流布されている DRDoS 攻撃用ツールを利用した。(このツールは予め作成した Reflector のリスト内のアドレス宛に、攻撃先のアドレスを送信元アドレスにセットした SYN パケットを送信することができる。)
- ・攻撃パケットは 50pps 送出。

(b) Reflector(踏み台)ホスト

以下の OS を Reflector に利用した。  
Win2000 [PC-K] × 8 台、 WinNT4.0 [PC-J] × 8 台  
RedHat [PC-H] × 8 台、 FreeBSD [PC-I] × 8 台  
Solaris [PC-M] × 8 台、 HP [PC-L] × 8 台  
IOS [RT-C] × 10 台

(c) 被攻撃側ファイアウォール

ステート情報にない SYN/ACK パケットを受信した際、破棄する (RST パケットを送出しない) ルールを設定した。

(4) 方法

検証環境下において DRDoS 攻撃用ツールを利用して、送信元アドレスを被攻撃ホストのアドレスに偽装した SYN パケットを Reflector(踏み台)ホスト宛に送出し、その反射 (SYN/ACK) パケットについての通信量を OS 別に測定した。

(5) 結果

ルータ間 (RT-A ~ RT-C) に設置したアナライザ (Analyzer) において、通信量を測定した結果を以下の図 2.15 に示す。OS により反射 (SYN/ACK) パケットの通信量が異なる結果となった。これは、OS により SYN/ACK パケットの再送回数が異なる実装となっていることに起因するものである。

しかし、いずれの OS においても攻撃用ホストが送信する SYN パケットが 50pps であるのに比べ、多いもので 20 倍を超える反射パケットが被攻撃側に送信さ

れることが分かる。

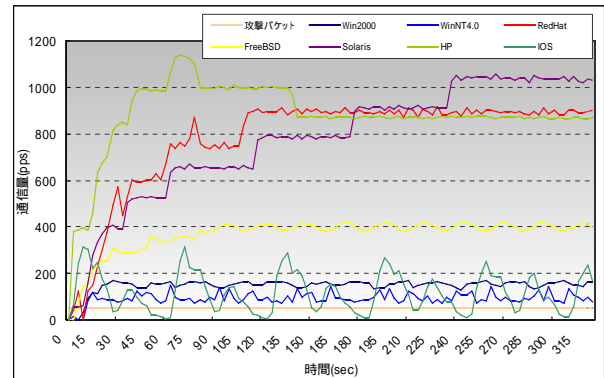


図 2.15 DRDoS パケット量の比較

(6) 考察

DRDoS 攻撃は、SYN/ACK パケットの再送というプロトコルの仕組みを巧みに利用し、パケット量を倍増させることにより、容易に回線の帯域を圧迫することができるものである。一般的な接続環境では自組織とその上流の間を結ぶ回線が細くなっていることが多いことから、DRDoS 攻撃によるネットワーク帯域消費は、特に自組織と上流のルータ間において最も深刻となる傾向がある。また、インターネットで公開されている多くのサーバやルータは、Reflector として悪用される危険性がある。

2.4.2 ネットワーク機器における各機能による防御について調査

(1) 概要

DRDoS 攻撃の性質に鑑みた対策について触れる。ルータの各機能による防御対策例を考え、それぞれについて調査した。

(2) 調査項目

(a) ルータにおけるアクセス制御

- ・送信元 IP アドレスを基に、reflector からのパケットを遮断。
- ・送信元ポートが特権ポートである SYN/ACK パケットを遮断。

(b) ルータにおける帯域制御

- ・CAR 機能を利用したポート別の帯域制御。

### (3) 結果

#### (a) reflector からのパケットをアクセス制御

攻撃を受けた際、有効な一時的回避策として、ルータによるアクセス制御を活用する手段がある。この手段は送信元により近い箇所にて対策を施す必要があるため、ISP など上流のルータ所有者に協力を要請し、SYN/ACK の送信元である Reflector からの通信を破棄するよう依頼する必要がある。これは実際の<sup>(注<sup>13</sup>)</sup>インシデント事例でとられた方法でもあり、効果があったと報告されている。

但し、ルータによるアクセス制御にも留意すべき点がある。即ち、攻撃実行者が予め複数の Reflector 群を用意し、それらを一定期間毎に切替えて攻撃を企てた場合(図 2.16 参照)、新たな Reflector に対しては脆弱なままとなってしまう。従って、そのような場合には Reflector の切替えに応じてその都度アクセス制御を行う必要性が生じる。

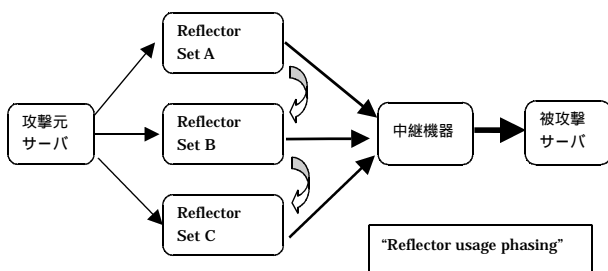


図 2.16 Reflector usage phasing 概念図

#### (b) 送信元ポートが特権ポートであるパケットをアクセス制御

一般的に Reflector として悪用されるマシンは特権ポート(1024 番未満のポート)において TCP のサービスを提供しているサーバであり、攻撃パケットは 1024 番未満のポートが送出元となる。他方、通常のパケットは短命ポート(1024 番以上のポート)から送出される。従ってこの点に着目し、ルータのアクセス機能を用いることで一定の範囲で攻撃を防御することが可能である。

保護したいサーバが Web サーバであった場合の具体的な方法として「外部の

ホストから DMZ 側に位置する Web サーバへの通信において、送信元ポートが特権ポートであり、送信先が Web サーバの 80/TCP 宛の接続をアクセス拒否」という方法がある。

但し、悪用されるサーバによっては特権ポート以外でも TCP サービスを提供しているものがあり、攻撃対象ホストからのアクセスにも制限がかかるため注意が必要である。

#### (c) CAR 機能を利用したポート別の帯域制御

前出の SYNflood 対策として挙げたルータの QoS 機能も有効な回避策となりうる。

### (4) 考察

DRDoS 攻撃の防御は、どの防御機能も十分なものとはならない。ただ、攻撃パケットの特徴をいち早く掴み、それを基に防御機能の選択・設定・調整を行うことにより、ある程度、被害を回避することは可能といえよう。

## 3. まとめ

DoS/DDoS 攻撃の脅威が現実の問題となっている中で、各企業では 1Gbps のトラフィックに対応したファイアウォールや DoS/DDoS 攻撃の防御機能を実装した各機器の導入が進んでいる。

2 章検証結果において、これら各機器に実装されている機能について有効性の検証を行った結果、個別の防御策を正確に選定し、講ずることにより、一定の効果が期待できることを確認した。

基本的な DoS/DDoS 攻撃の防御対策は、ボーダールータやファイアウォールなどのセキュリティ機能を利用し不要なパケットを削除することである。さらに、システムや各機器が許容する通信量を超えないよう帯域を制御することである。

次に、DoS/DDoS 攻撃に利用されるパケットの特徴(プロトコル、パケット長及びパケット量等)と各防御機能の特徴に鑑み、整理を行うことにより適切な防御策を講じることができるといえる。各防御機能の特徴を理解する為には、各機

器の限界(例えば、ハーフオープン最大数、コネクション最大数、各タイムアウト時間、各リトライ数、サービス処理能力及び回線容量等)を事前に把握することが必要である。これは、各機器の設定を行う上で、該当機能を正確に動作させることにも繋がる。

大事なことは、技術を正しく理解して、正しく運用することである。

実際にサービス不能の事態に陥った場合は、まず攻撃を受けているのかアクシデントなのか判断する。攻撃を受けているのであれば、通信内容、各機器の状態及び負荷状況等から攻撃の種類を迅速に判断し、攻撃の性質、特徴に合った対応を実施しなければならない。

この際においても、各機器の機能や性能を考慮し適切に対処することが肝要であり、適切な判断を行える体制の整備が必要となる。対策決定においては、サービスを制限することによるユーザの利便性の損失とシステム所有者の利益損失や社会的影響を踏まえ、提供しているサービスを制限するのか、一時停止することも考慮するのかなどについて考慮することが重要である。そのためには、インシデントが発生した場合の対応手順を事前に策定しておくなど、インシデントレスポンスやリスクマネジメントなどの観点を含め、システムの包括的な安全対策の構築をすることが求められる。

#### 脚注

(注 1) syncookies ... TCP のスリーウェイ・ハンドシェイクにおいて、SYN/ACK パケットの TCP 初期シーケンス番号(ISN)を記憶せず、SYN パケットの送信元の IP アドレス、ポート、シーケンス及び時間によって変化する変数の値を基に一方ハッシュ関数(MD5)を用いて算出した番号(これをクッキーと呼ぶ)を、TCP 初期シーケンス番号(ISN)に設定した SYN/ACK パケットを送信する。ACK パケットを受信すると、再び同様の方法でクッキーを算出し、その値に 1 を加えた値が ACK パケットの ACK 番号に一致しておればハンドシェイク成功とみなす仕組み。

(注 2) 別紙主要機器諸元参照

(注 3) pps ... pps ( packet per second の略 )  
1 秒間あたりに転送(送信)できるパケット量

のこと。

(注 4) iptables を無効... iptables を利用しリミットをかける SYNflood の防御方法もあるが、本検証では対象外とした。

(注 5) tcp\_max\_syn\_backlog ... 送信した SYN のステートを記憶する最大数の設定

(注 6) tcp\_synack\_retries ... SYN/ACK の再送回数の設定

(注 7) tcp\_abort\_on\_overflow ... listen 状態のサービスに、新しいコネクションの受け入れ(accept)が非常に遅い場合、それらをリセットするか否かの設定

(注 8) SYN Flood Protection 機能... Netscreen 社製ファイアウォール Netscreen に実装されている SYNflood 防御機能であり、1 秒あたりの SYN パケットの通過パケット数が閾値を超過すると、接続元からの通信に対してファイアウォールが TCP レベルの代理応答を行う。今回は検証上、常に動作状態にするため、閾値を 1pps とした。

(注 9) CAR(Committed Access Rate) 技術

単位時間あたり一定量以上のパケットがルータに入ってくる場合、一定以上のパケットを制限する技術。

(注 10) FlameThrower

アプリケーションプロトコルエミュレータ、DoS/DDoS エミュレータ及びパケットジェネレータ機能を持つなど、TCP/IP の全てのレイヤーレベルでエミュレートする装置。サーバ、ファイアウォール又はネットワークデバイス等の性能評価試験で広く利用されている。

<http://www.antara.net/>

(注 11) FlameThrower に付属するパケットジェネレータ

(注 12) UDPFlood 拒否機能...単一又は複数のソースアドレスから 1 アドレス宛への UDP パケットの通信を、閾値以上と検知した場合、UDPFlood があつたとみなしファイアウォールは約 1 秒間、UDP パケットを拒否する機能。

(注 13) The Distributed Reflection DoS Attack  
<http://grc.com/dos/drdo.htm>

#### 参考文献

(1) RedHat Linux 参照ガイド

<http://www.jp.RedHat.com/manual/Doc9/rhl-rg-ja-9/index.html>

(2) Solaris Operating Environment Network Settings for Security - Updated for Solaris 8 Operating Environment  
<http://www.sun.com/blueprints/1200/network-updt1.pdf>

(3) Solaris カーネルのチューンアップ・リファレンスマニュアル  
<http://docs-pdf.sun.com/816-3961/816-3961.pdf>

(4) Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks  
[http://www.cisco.com/warp/public/707/new\\_sflash.pdf](http://www.cisco.com/warp/public/707/new_sflash.pdf)

(5) Rate Limiting for TCP SYN Packets  
[http://www.cisco.com/warp/public/63/car\\_rate\\_limit\\_icmp.pdf](http://www.cisco.com/warp/public/63/car_rate_limit_icmp.pdf)

(6) QoS Frequently Asked Questions  
[http://www.cisco.com/warp/public/105/qos\\_faq.pdf](http://www.cisco.com/warp/public/105/qos_faq.pdf)

(7) The Distributed Reflection DoS Attack  
<http://grc.com/dos/drdo.htm>

(8) distributed attack tools  
<http://packetstormsecurity.nl/distributed/>

(9) Help Defeat Denial of Service Attacks: Step-by-Step  
<http://www.sans.org/dosstep/>

(10) W. Richard Stevens 「詳解 TCP/IP Vol.1 プロトコル」 ピアソン・エデュケーション(2000.12)

(11) Gary R. Wright, W.Richard Stevens 「詳解 TCP/IP Vol.2 実装」 ピアソン・エデュケーション(2002.12)

(12) Gian Paolo D. Musumeci, Mike Loukides 「Unix システムパフォーマンスチューニング 第2版」 オライリージャパン

(13) Kevin Mandia, Chris Prosise 「インシデント レスポンス」 翔泳社

(14) Srinivas Vegesna 「IP QoS 完全ガイド」 ソフトバンクパブリッシング

別紙：主要機器諸元

表 2.4 主要機器諸元表

名称	IP アドレス	CPU	Memory	OS
PC-A	172.16.1.52/24	Pentium (1.0GHz)	128MB	Windows2000 Pro.
PC-B	172.16.1.53/24	Pentium (1.0GHz)	512MB	Windows2000 Server
PC-C	172.16.1.54/24	Pentium (1.0GHz)	512MB	RedHat 7.1
PC-D	172.16.5.56/24 172.16.5.57/24	Pentium (1.0GHz)	512MB	RedHat 9
PC-E	172.16.1.222/24	Pentium (1.0GHz)	512MB	Windows2000 Pro.
PC-F	172.16.5.60/24	Ultra SPARC- (400MHz)	512MB	Solaris 9
PC-G	172.16.5.61/24	Ultra SPARC- (400MHz)	512MB	Solaris 9
PC-H	172.20.26.1 ~ 4/24 172.20.27.1 ~ 4/24	Pentium (1.0GHz)	512MB	RedHat 7.2
PC-I	172.20.28.1 ~ 4/24 172.20.29.1 ~ 4/24	Pentium (1.0GHz)	512MB	FreeBSD 4.4
PC-J	172.20.24.1 ~ 4/24 172.20.25.1 ~ 4/24	Pentium (1.0GHz)	512MB	WindowsNT4.0
PC-K	172.20.22.1 ~ 4/24 172.20.23.1 ~ 4/24	Pentium (1.0GHz)	512MB	Windows2000
PC-L	172.20.32.1 ~ 4/24 172.20.33.1 ~ 4/24	PA8500(440MHz)	512MB	HP-UX11
PC-M	172.20.30.1 ~ 4/24 172.20.31.1 ~ 4/24	Ultra SPARC- (450MHz)	512MB	Solaris8
PC-N	172.16.5.58/24	Pentium (1.0GHz)	512MB	RedHat 9

名称	品名	Memory	OS
Analyzer	Surveyor	512MB	Windows2000 Pro.
F/W	Netscreen100 110(0)-(11)	48MB	ScreenOS4.0.0r11.0
RT-A	CISCO7507	64MB	IOS12.1(10)E
RT-B	CISCO7507	64MB	IOS12.1(10)E
RT-C	CISCO3640	32MB	IOS12.1(5)TQ
LB	CISCO LD430	384MB	3.2.3