DoS 保護の設定

この章では、DoS 攻撃（サービス拒絶攻撃）からシステムを保護する方法について説明します。この章の情報は Cisco 7600 シリーズ ルータ固有であり、このマニュアルの「ネットワーク セキュリティの設定」で説明したネットワーク セキュリティ情報と手順、および次のマニュアルで説明されているネットワークセキュリティ情報と手順を補います。

- 次の URL の『*Cisco IOS Security Configuration Guide*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm
- 次の URL の『*Cisco IOS Security Command Reference*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

この章で説明する内容は、次のとおりです。

DoS 保護の概要

Cisco 7600 シリーズ ルータで使用できる DoS 保護では、2 種類の DoS 攻撃シナリオに対するサポートを提供します。

- ルーティングプロトコル処理容量を不足させるデータパケット処理により、次のような DoS 攻撃を受ける場合があります。
  - hello タイムアウトによるルーティング ピア損失
  - hello タイムアウトによる HSRP ピア損失
  - ルーティング プロトコルの低速なコンバージェンス
- CPU インバンド データパスを輻輳させるデータ パケットにより、次のような DoS 攻撃を受ける場合があります。
  - hello パケット ドロップによるルーティング ピア損失
  - hello パケット ドロップによる HSRP ピア損失

（注） ローカル ルータで使用される DoS 保護は、外部リンク上のデータパケット輻輳に起因するピア損失を防止できません。

DoS 保護の設定

ここでは、各種 DoS 保護の実装について説明し、設定例を示します。

スーパーバイザ エンジンの DoS 保護

スーパーバイザ エンジンでは、トラフィック レートを制限するメカニズムがハードウェアに組み込まれており、ルート プロセッサのフラッディングおよび DoS を防止します。レート制限により、大部分のトラフィックをハードウェアでドロップし、少量のトラフィックのみを 0.5 パケット / 秒という設定変更不可能なレートでルート プロセッサに転送できます。ハードウェアでのパケットのレート制限では、次のようなトラフィックを処理します。

- ACL 拒否用の Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）到達不能メッセージ

  この条件により、ACL で拒否されたパケットの大部分をハードウェアでドロップし、一部のパケットをモニタリング用にルート プロセッサに転送できます。

（注）　システムでは ACL 拒否ログ パケットをすべてルート プロセッサにブリッジングするようプログラムされているため、セキュリティ ACL に拒否ログ ACE を設定しないことを推奨します。

- ICMP リダイレクト メッセージ

  ICMP リダイレクト メッセージは、データ リンク上のホストに特定の送信先へのより優れたルートが使用可能であることを通知するために、ルータにより使用されます。大部分のメッセージはハードウェアでドロップされ、ルート プロセッサに到達する必要があるメッセージはごくわずかです。

- Fowarding Information Base（FIB; 転送情報ベース）の障害

  FIB が特定の宛先 IP アドレスへのルーティング方法を認識していない場合は、一部のパケットがルート プロセッサに転送され、ICMP リダイレクト メッセージを生成します。

- Reverse Path Fowarding（RPF）の障害

  FIB 送信元 IP アドレス ルックアップにより RPF 障害が生じた場合、一部のパケットがルート プロセッサに転送され、ICMP 到達不能メッセージを生成します。

セキュリティ ACL

Cisco 7600 シリーズ ルータは、セキュリティ ACL を使用することによりハードウェアでパケットを拒否し、DoS パケットが CPU インバンド データパスに到達する前にドロップできます。セキュリティ ACL は、ハードウェア内で TCAM を使用して適用されるため、他のトラフィックのスループットに影響を及ぼすことなく、長いセキュリティ ACL が使用できます。また、セキュリティ ACL は DoS 攻撃が識別されたあとでも適用できます。

セキュリティ ACL を使用して DoS パケットをドロップする際、次の点に注意してください。

- セキュリティ ACL は、ドロップされるトラフィック フローを指定する必要があります。
- すでにセキュリティ ACL が設定されているインターフェイスにセキュリティ ACL を追加して、DoS パケットをブロックする場合は、既存のセキュリティ ACL と DoS セキュリティ ACL を 1 つにまとめる必要があります。
- セキュリティ ACL は、保護を必要とするすべての外部インターフェイス上で設定する必要があります。複数のインターフェイス上でセキュリティ ACL を設定するには、インターフェイス レンジ コマンドを使用します。

次に、セキュリティ ACL を使用して DoS パケットをドロップする例を示します。

```
Router# clear mls ip mod 9
Router# show mls ip mod 9
Displaying Netflow entries in module 9
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
199.1.1.1       199.2.1.1       0   :0      :0        0   : 0
1843         84778       2     02:30:17   L3 - Dynamic
199.2.1.1       199.1.1.1       0   :0      :0        0   : 0
2742416      126151136   2     02:30:17   L3 - Dynamic          トラフィック フローの識別
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no access-list 199
Router(config)# access-list 199 deny ip host 199.1.1.1 any
Router(config)# access-list 199 permit ip any any
Router(config)# interface g9/1
Router(config-if)# ip access 199 in                          セキュリティ ACL の適用
Router(config-if)# end
Router#
1w6d: %SYS-5-CONFIG_I: Configured from console by console
Router# clear mls ip mod 9
Router# show mls ip mod 9
Displaying Netflow entries in module 9
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
199.1.1.1       199.2.1.1       0   :0      :0        0   : 0
1542         70932       2     02:31:56   L3 - Dynamic
199.2.1.1       199.1.1.1       0   :0      :0        0   : 0
0            0           2     02:31:56   L3 - Dynamic          ハードウェア転送トラフィックの停止
Extended IP access list 199
    deny ip host 199.1.1.1 any (100 matches)
    permit ip any any
Router# show access-list 199
Extended IP access list 199
    deny ip host 199.1.1.1 any (103 matches                  0.5 pps でのレート制限
    permit ip any any
Router #
```

QoS ACL

セキュリティ ACL と異なり、QoS ACL を使用すると、フローのすべてのトラフィックへのアクセスを拒否することなく、トラフィック レートを制限できます。

QoS ACL を使用してパケットのレートを制限する際、次の点に注意してください。

- QoS ACL は、レート制限されるトラフィック フローを指定する必要があります。
- すでに QoS ACL が設定されているインターフェイスに QoS ACL を追加して、パケットのレートを制限する場合は、既存の QoS ACL とレート制限 ACL を 1 つにまとめる必要があります。
- QoS ACL は、保護を必要とするすべての外部インターフェイス上で設定する必要があります。複数のインターフェイス上で ACL を設定するには、インターフェイス レンジ コマンドを使用します。

次に、QoS ACL を使用してルータ上の Ping 攻撃を防止する例を示します。QoS ACL をすべてのインターフェイスに設定および適用することで、着信 ICMP エコー パケットのレートを制限します。

```
Router# show ip ospf neighbors

Neighbor ID     Pri   State           Dead Time   Address         Interface
6.6.6.122         1   FULL/BDR        00:00:30    6.6.6.122       Vlan46
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                          (sec)         (ms)       Cnt Num
0   4.4.4.122               Vl44          11 00:06:07    4   200  0  6555
Router#                                                          ping 攻撃の開始
Router# show proc cpu | include CPU utilization
CPU utilization for five seconds: 99%/90%; one minute: 48%; five minutes: 25%
Router#
2w0d: %OSPF-5-ADJCHG: Process 100, Nbr 6.6.6.122 on Vlan46 from FULL to DOWN, Neighbor Down:
Dead timer expired
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# access-list 199 permit icmp any any echo
Router(config)# class-map match-any icmp
Router(config-cmap)# match access-group  199
Router(config-cmap)# exit
Router(config)# policy-map icmp
Router(config-pmap)# class icmp
Router(config-pmap-c)# police 96000 16000 16000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface range g4/1 - 9
Router(config-if-range)# service-policy input icmp                  ポリシーの適用
Router(config-if-range)# end
2w0d: %SYS-5-CONFIG_I: Configured from console by console
2w0d: %OSPF-5-ADJCHG: Process 100, Nbr 6.6.6.122 on Vlan46 from LOADING to FULL, Loading Done
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                          (sec)         (ms)       Cnt Num
0   4.4.4.122               Vl44          13 00:00:48    8   200  0  6565
Router#
```

FIB レート制限

FIB レート制限により、ソフトウェア処理を必要とするすべてのパケットをレート制限することができます。

FIB レート制限を使用する際には、次の点に注意してください。

- FIB レート制限は、マルチキャスト トラフィックを制限しません。
- FIB レート制限は、正当なトラフィックと不正なトラフィックを区別しません（トンネル、Telnet など）。
- FIB レート制限では、フロー単位のレート制限ではなく、集約レート制限が適用されます。

次に、ローカル接続されたサブネット上の存在しないホスト アドレスを宛先とするトラフィックの例を示します。通常、Address Resolution Protocol（ARP; アドレス解決プロトコル）要求に対して ARP 応答が返され、このトラフィックの FIB 隣接関係が確立されます。ただし、この宛先サブネットの FIB 隣接関係では、トラフィックを受信して、これをソフトウェア処理用に転送するという作業をし続けることになります。このトラフィックにレート制限を適用することにより、ソフトウェア処理用に転送されるトラフィックのレートを管理可能な量にまで制限できます。

```
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   4.4.4.122               Vl44          11 00:00:26    8   200  0  6534
Router# show ip ospf neighbors

Neighbor ID     Pri   State           Dead Time   Address         Interface
6.6.6.122         1   FULL/BDR        00:00:36    6.6.6.122       Vlan46
→ Router#                                                  攻撃の開始
Router# show arp | include 199.2.250.250
Internet  199.2.250.250           0   Incomplete      ARPA
Router#
1w6d: %OSPF-5-ADJCHG: Process 100, Nbr 6.6.6.122 on Vlan46 from FULL to DOWN, Neighbor
Down: Dead timer expired
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
→ Router(config)# mls ip cef rate-limit 1000          1000 pps でのトラフィック  レート制限
Router(config)# end
Router#
1w6d: %SYS-5-CONFIG_I: Configured from console by console
Router#
1w6d: %OSPF-5-ADJCHG: Process 100, Nbr 6.6.6.122 on Vlan46 from LOADING to FULL,
Loading Done
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   4.4.4.122               Vl44          12 00:00:07   12   200  0  6536
Router#
```

ARP スロットリング

ARP スロットリングでは、接続ネットワークを宛先とするパケットがルート プロセッサに転送されるレートを制限します。これらのパケットの大部分はドロップされますが、少数のパケットはルータに送信されます（レート制限）。

パケット ドロップ統計情報のモニタリング

レート制限メカニズムでは一定数のパケットがソフトウェア処理用に転送されるため、CLI から NetFlow **show** コマンドを入力することにより、パケット ドロップ統計情報を表示できます。また、インターフェイス上の着信または発信トラフィックをキャプチャし、このトラフィックのコピーを外部インターフェイスに送信して、トラフィック アナライザなどによりモニタリングすることもできます。トラフィックをキャプチャし、外部インターフェイスに転送するには、**monitor session** コマンドを使用します。

NetFlow コマンドによるドロップされたパケットのモニタリング

ルータ MAC を宛先とし、ルート プロセッサにハードウェア スイッチングまたはハードウェア転送された フローを表示するには、次の Netflow コマンドを使用します。

MLS NetFlow フローマスクが destination-only よりも大きい値に設定されている場合に限り、送信元またはフローに基づく統計情報が表示されます。

```
Router# show mls ip
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
200.2.5.3       0.0.0.0         0   :0      :0        0  : 0

Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
0            0           1     01:52:25   L3 - Dynamic

Router# show mls netflow flowmask
 current ip flowmask for unicast: destination only
 current ipx flowmask for unicast: destination only

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls flow ip destination-source
Router(config)# exit
1w6d: %SYS-5-CONFIG_I: Configured from console by console
Router# show mls ip
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
200.2.5.3       223.255.254.226 0   :0      :0        0      : 0
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
0            0           2     01:54:05   L3 - Dynamic

Router#
```

show mls ip コマンドを使用して特定の送信元アドレスまたは宛先アドレスを持つフロー情報を表示する場合、このコマンドには 32 ホスト プレフィクスのみを指定できます。出力修飾子を使用すると、特定のサブネットからのすべてのフローが表示されます。

```
Router# show mls ip source 9.9.9.2 mod 4
Displaying Netflow entries in module 4
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
9.9.9.177       9.9.9.2         0   :0      :0        0      : 0
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
0            0           28    01:56:59   L3 - Dynamic

Router# show mls ip mod 4 | include 9.9.9
9.9.9.177       9.9.9.2         0   :0      :0        0   : 0
9.9.9.177       9.9.9.1         0   :0      :0        0   : 0
```

monitor session コマンドによるドロップされたパケットのモニタリング

次に、**monitor session** コマンドを使用して、トラフィックをキャプチャし、外部インターフェイスに転送する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 source vlan 44 both
Router(config)# monitor session 1 destination interface g9/1
Router(config)# end
Router#
2w0d: %SYS-5-CONFIG_I: Configured from console by console
Router# show monitor session 1
Session 1
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          44
Destination Ports: Gi9/1
Filter VLANs:      None
```