FIREWALL設定

ファイアウォール処理による転送動作

SRXは、用途によってパケットの転送方法をデバイス単位で選択する事が出来ます。

- Flow-based forwarding: ステートフルインスペクション
- Packet-based forwarding: 通常のルータ/SW動作

SRXをFW/VPN機器として利用する場合には、フローベースフォワーディングを選択します。

フローベースフォワーディングはディフォルトで設定されています。

【 参考: SRX製品毎の転送モード対応状況(10.2) 】

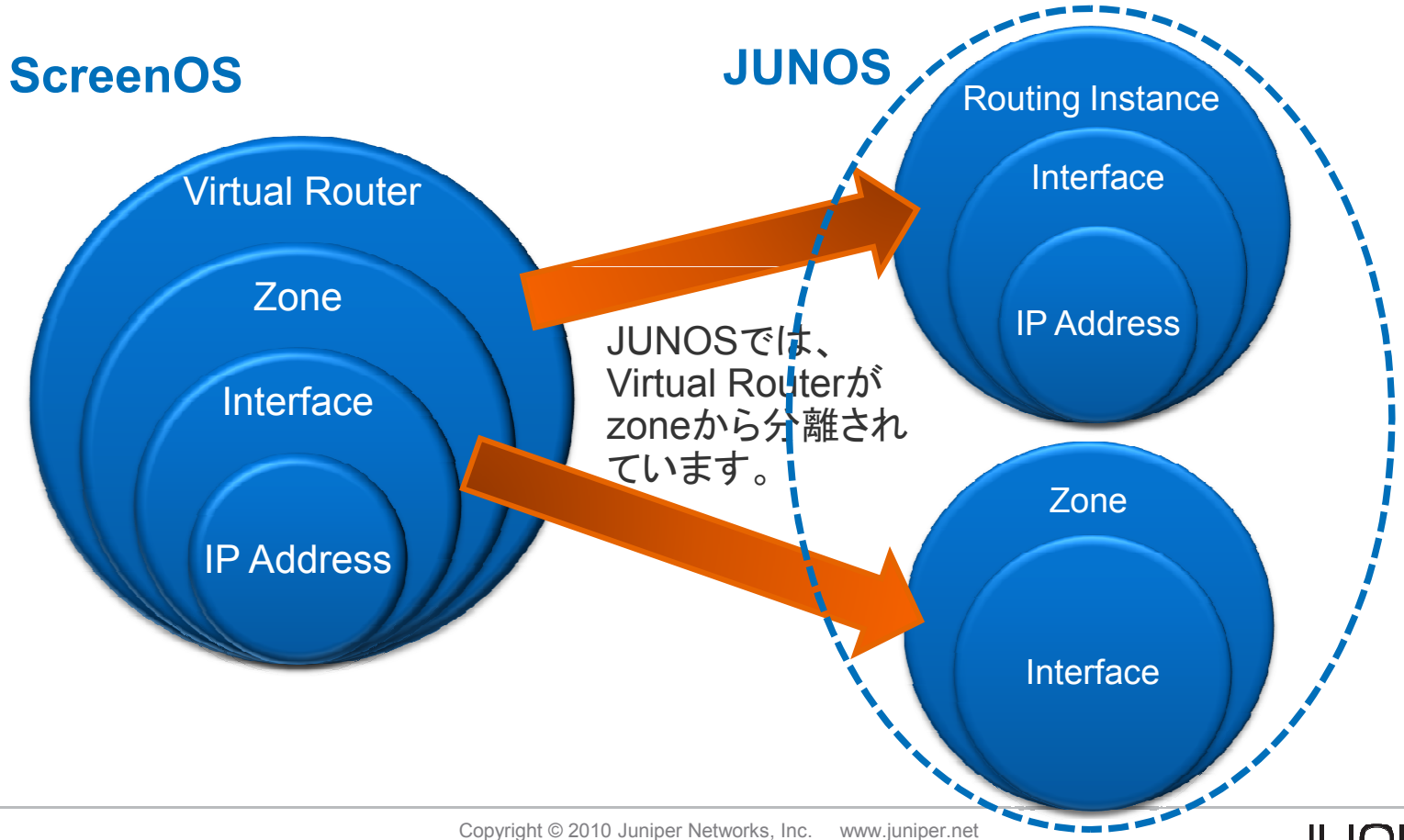
	Route/Nat (L3/L4)		Bridge (L2)	
	Flow-based	Packet-based	Flow-based (Transparent Mode)	Packet-based (Ethernet Switching)
SRX100/210/240/650	対応（default）	対応	未対応（将来対応予定）	対応
SRX5000/3000	対応	未対応	対応	未対応

* ScreenOSでは、Flow-based forwardingのみに対応

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

ゾーン、インタフェースの考え方 – SCREENOSとの違い

複数のフォワーディングモードを持つことから、SRXでは論理的な設定対象の考え方がScreenOSと異なり、フォワーディング関連の設定対処とセキュリティ系の設定対象が分離されています。



Copyright © 2010 Juniper Networks, Inc.

バーチャルルータの設定例

```
interfaces {
      ge-0/0/2 {
          unit 0 {
                 family inet {
                     address 192.168.1.2/24;
                 }
           }
      }
}
routing-instances {
    vr1 {
        instance-type virtual-router;
        interface fe-0/0/2.0;
    }
}
```

← ロジカルインタフェースのvirtual-routerへバインド

ディフォルトで全てのインタフェースは、マスタルータ（ipv4ではinet.0）にバインドされており、複数のVR利用が不要であれば特に新しいVRを作成する必要はありません。）

Copyright © 2010 Juniper Networks, Inc.

セキュリティゾーンとは?

セキュリティゾーンとは、インタフェースに割り当てる仮想的なグループです。

SRXでは主にセキュリティゾーンを使ってトラフィックを制御します。トラフィック制御に用いるポリシー(後述)でチェックするのは入力ゾーンから違うゾーンへの通信もしくは入力ゾーンと同じゾーンの場合のトラフィックです。

セキュリティゾーンは、下記の二つのタイプが存在します。

- Functional zone
  主にManagementの為のゾーンで、本ゾーンで受信したトラフィックが転送されることはありません。SRXでは、ScreenOSと異なり、多くの機器に専用管理インタフェースとなるfxp0が提供されていることもあり、ほとんどの場合でFunctional zoneを意識する必要はありません。
- Security zone
  FWを通過するトラフックに対して制御するためのゾーン。通常ゾーンといった場合には、このセキュリティゾーンを示します。FWポリシーは、セキュリティゾーン間で設定されることになります。
  - SRXでは、デフォルトのSecurity Zoneとして以下が初めから定義されています。
    - Null-Zone: デフォルトのゾーン。全てのトラフィックはドロップされる。
    - junos-global: SRX内部で用いられる論理的なゾーン。通常は特に存在を意識する必要無し。

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

ゾーンの設定例 – SRX100デフォルトでの設定

```
security {
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                vlan.0;
            }
        }
        security-zone untrust {
            screen untrust-screen;
            interfaces {
                fe-0/0/0.0 {
                    host-inbound-traffic {
                        system-services {
                            dhcp;
                            tftp;
                        }
                    }
                }
            }
        }
    }
}
```

他のポートはbridge portとしてtrust zoneへ割り当て

WANポートのみ、untrust zoneへ割り当て

Copyright © 2010 Juniper Networks, Inc.

ゾーンの設定例 – SRX100デフォルトでの設定

```
lab# run show security zones

Security zone: trust
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    vlan.0

Security zone: untrust
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Screen: untrust-screen
  Interfaces bound: 1
  Interfaces:
    fe-0/0/0.0
```

既存のセッションにマッチしないTCP SYNパケットを受信した場合、RSTを返す

本ゾーンに対してポリシーが設定されているか

本ゾーンに適用されているScreen防御の設定名（後述）

本ゾーンにバインドされているインタフェース

Copyright © 2010 Juniper Networks, Inc.

ゾーンの設定 (HOST-INBOUND-TRAFFIC)

SRX自終端トラフィックについて

- 自終端トラフィックは、host-inbound-trafficによりzoneまたはインタフェース毎にフィルタ制御されます。
- 自終端のサービスそのものの起動有無は、system → services 配下で設定されます。
- system-services
  - 該当zone(interface)で送受信を許容するサービスを指定します。
- protocols
  - 該当zone(interface)で送受信を許容するプロトコルを指定します。
- 本設定にて指定されていないサービスとプロトコルパケットで、該当するzone(interfaces)を経由するトラフィックは全てdropされます。
- 自終端サービスの送信元（例：Telnet/J-Web等）IPを制限したい場合には、L3 Firewall FilterをIo0.0に設定します。

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

参考 – デフォルト起動サービス

```
system {
    services {
        ssh;
        telnet;
        xnm-clear-text;
        web-management {
            http {
                interface vlan.0;
            }
            https {
                system-generated-certificate;
                interface vlan.0;
            }
        }
        dhcp {
            router {
                192.168.1.1;
            }
            pool 192.168.1.0/24 {
                address-range low 192.168.1.2 high 192.168.1.254;
            }
            propagate-settings fe-0/0/0.0;
        }
    }
}
```

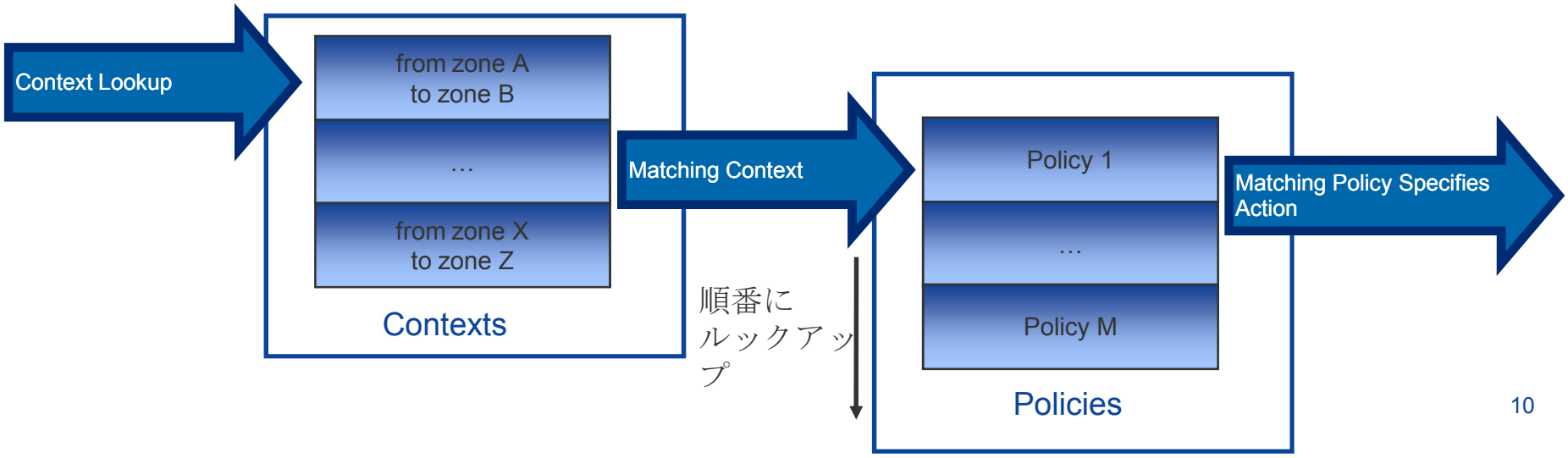

Copyright © 2010 Juniper Networks, Inc.

セキュリティポリシーとは?

セキュリティゾーン間を跨ぐ(SRXを通過する)通信を制御するためのポリシールールです。

本設定により、FW/VPN(IPSEC)などのトラフックが制御可能になります。

ScreenOSでは、NATルールの記述も合わせてポリシーにて行われていましたが、SRXでは、NATは別ルールにて記述されます。



Copyright © 2010 Juniper Networks, Inc. www.juniper.net

ポリシー関連スケーラビリティ数

	SRX100 (LM/HM)	SRX210 (LM/HM)	SRX240 (LM/HM)	SRX650
Max Sessions	16000/32000	32000/64000	64000/128000	512000
Virtual Routers	3	10	20	60
VLANs	16	64	512	4096
IFLs（論理IF）	64	100	256	2048
Max Policies	384	512	4096	8192
Max Policies w/ Count	128	128	256	256
Security Zones	10	12	32	128
Address Book	512/1024	512/1024	1024/2048	2048
Address Set	128	128	128	128
Addresses per Policy	512	512	512	512

Copyright © 2010 Juniper Networks, Inc.

セキュリティポリシー設定の手順

1. セキュリティポリシーオブジェクトの設定
   - Security zones の設定
   - Address-Book の登録（オプション）
   - Custom-Applicationの登録（オプション）
   - Schedulerの登録（オプション）
2. ALG の設定（オプション）
3. セキュリティポリシーの記述
   - From-zone / to-zoneの指定
   - Match criteria の指定
     - Addresses/Address sets (source/destination)
     - Applications/Application sets
   - Action の指定
     - Permit / Deny / Reject
     - Log（オプション）
     - Count（オプション）

Permitアクション時の追加オプション	
firewall-authentication	FW認証処理
application-services	UTM/IDP/GPRS等より上位セキュリティチェック処理
destination-address	宛先NAT処理
tunnel	ポリシーベースIPsec VPN処理

Copyright © 2010 Juniper Networks, Inc.

アドレスブックの登録（オプション）

ポリシールール内の source/destination address にて使用するaddressを指定し登録します。

すべてのトラフィックを通過させたい場合は、予め定義されている any を選択してください。

Copyright © 2010 Juniper Networks, Inc.

アドレスブック設定例

```
security {
    zones {
        security-zone trust {
            address-book {
                address host.251 192.168.1.251/32;
                address 192.168.1.252/32 192.168.1.252/32;
                address http_server1 {
                    dns-name www.testhogehoge.com;
                }
            }
          security-zone untrust {
              address-book {
                  address 100.100.100.0/24 100.100.100.0/24;
                  }
        }
}
```

← DNS Nameでのアドレス指定

Copyright © 2010 Juniper Networks, Inc.

プリディファインドアプリケーション

SRXでは、ウェルノウンポートに従い、多くのアプリケーションがpredefined service として登録されています。

- Predefined service は、以下コマンドにて確認が出来ます。
  (config-mode)# show groups junos-defaults applications

事前定義されているアプリケーションは全て ”junos-” から始まります。

事前定義アプリケーションはデフォルトで”junos-defaults” グループに属し、CLIから確認できます。

事前定義アプリケーションは “any” に全てマッチします。

事前定義とカスタムで作成したApplicationをグループ化することも可能です。

Copyright © 2010 Juniper Networks, Inc.

プリディファインドアプリケーション　例

```
lab# show groups junos-defaults applications | hold
#
# File Transfer Protocol
#
application junos-ftp {
    application-protocol ftp;
    protocol tcp;
    destination-port 21;
}
#
# Trivial File Transfer Protocol
#
application junos-tftp {
    application-protocol tftp;
    protocol udp;
    destination-port 69;
}
#
# Real Time Streaming Protocol
#
application junos-rtsp {
    application-protocol rtsp;
    protocol tcp;
    destination-port 554;
}
#
# Network Basic Input Output System  - networking protocol used on
# Windows networks   session service port
#
application junos-netbios-session {
    protocol tcp;
    destination-port 139;
}
.
.
.
```


Copyright © 2010 Juniper Networks, Inc.

参考：プリディファインドアプリケーションのタイムアウト値 – TCP 1/4

```
tcp port=0, appl_name=junos-tcp-any, service type=0, alg id=0, timeout=1800
tcp port=21, appl_name=junos-ftp, service type=1, alg id=1, timeout=1800
tcp port=22, appl_name=junos-ssh, service type=22, alg id=0, timeout=1800
tcp port=23, appl_name=junos-telnet, service type=10, alg id=0, timeout=1800
tcp port=25, appl_name=junos-smtp, service type=7, alg id=0, timeout=1800
tcp port=43, appl_name=junos-whois, service type=46, alg id=0, timeout=1800
tcp port=49, appl_name=junos-tacacs, service type=0, alg id=0, timeout=1800
tcp port=53, appl_name=junos-dns-tcp, service type=16, alg id=16, timeout=1800
tcp port=65, appl_name=junos-tacacs-ds, service type=0, alg id=0, timeout=1800
tcp port=70, appl_name=junos-gopher, service type=39, alg id=0, timeout=1800
tcp port=79, appl_name=junos-finger, service type=17, alg id=0, timeout=1800
tcp port=80, appl_name=junos-http, service type=6, alg id=0, timeout=1800
tcp port=110, appl_name=junos-pop3, service type=8, alg id=0, timeout=1800
tcp port=111, appl_name=junos-sun-rpc-tcp, service type=5, alg id=5, timeout=2400
tcp port=113, appl_name=junos-ident, service type=34, alg id=0, timeout=1800
tcp port=119, appl_name=junos-nntp, service type=35, alg id=0, timeout=1800
tcp port=135, appl_name=junos-ms-rpc-tcp, service type=55, alg id=55, timeout=60
tcp port=139, appl_name=junos-smb, service type=21, alg id=0, timeout=1800
tcp port=143, appl_name=junos-imap, service type=9, alg id=0, timeout=1800
tcp port=179, appl_name=junos-bgp, service type=0, alg id=0, timeout=1800
tcp port=210, appl_name=junos-wais, service type=0, alg id=0, timeout=1800
tcp port=389, appl_name=junos-ldap, service type=47, alg id=0, timeout=1800
tcp port=443, appl_name=junos-https, service type=58, alg id=0, timeout=1800
tcp port=444, appl_name=junos-snpp, service type=0, alg id=0, timeout=1800
tcp port=445, appl_name=junos-smb, service type=21, alg id=0, timeout=1800
tcp port=514, appl_name=junos-rsh, service type=2, alg id=2, timeout=1800
tcp port=515, appl_name=junos-printer, service type=38, alg id=0, timeout=1800
tcp port=517, appl_name=junos-talk, service type=65, alg id=65, timeout=1800
tcp port=518, appl_name=junos-ntalk, service type=65, alg id=65, timeout=1800
tcp port=522, appl_name=junos-h323, service type=0, alg id=0, timeout=1800
tcp port=554, appl_name=junos-rtsp, service type=11, alg id=11, timeout=1800
tcp port=646, appl_name=junos-ldp-tcp, service type=0, alg id=0, timeout=1800
tcp port=705, appl_name=junos-snmp-agentx, service type=0, alg id=0, timeout=7560
tcp port=993, appl_name=junos-imaps, service type=0, alg id=0, timeout=1800
tcp port=1433, appl_name=junos-ms-sql, service type=56, alg id=0, timeout=1800
tcp port=1494, appl_name=junos-winframe, service type=78, alg id=0, timeout=1800
tcp port=1503, appl_name=junos-h323, service type=0, alg id=0, timeout=1800
tcp port=1521, appl_name=junos-sqlnet-v2, service type=64, alg id=64, timeout=1800
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

参考：プリディファインドアプリケーションのタイムアウト値 – TCP 2/4

```
tcp port=1525, appl_name=junos-sqlnet-v1, service type=0, alg id=0, timeout=1800
tcp port=1720, appl_name=junos-h323, service type=60, alg id=60, timeout=1800
tcp port=1723, appl_name=junos-pptp, service type=69, alg id=69, timeout=1800
tcp port=1731, appl_name=junos-h323, service type=0, alg id=0, timeout=1800
tcp port=1863, appl_name=junos-msn, service type=41, alg id=0, timeout=1800
tcp port=2000, appl_name=junos-sccp, service type=71, alg id=71, timeout=1800
tcp port=2049, appl_name=junos-nfsd-tcp, service type=0, alg id=0, timeout=1800
tcp port=2401, appl_name=junos-cvspserver, service type=0, alg id=0, timeout=1800
tcp port=3220, appl_name=junos-xnm-ssl, service type=0, alg id=0, timeout=1800
tcp port=3221, appl_name=junos-xnm-clear-text, service type=0, alg id=0,
timeout=1800
tcp port=3478, appl_name=junos-stun, service type=0, alg id=0, timeout=1800
tcp port=3479, appl_name=junos-stun, service type=0, alg id=0, timeout=1800
tcp port=3578, appl_name=junos-wxcontrol, service type=0, alg id=0, timeout=7560
tcp port=5050, appl_name=junos-ymsg, service type=33, alg id=0, timeout=1800
tcp port=5060, appl_name=junos-sip, service type=63, alg id=63, timeout=1800
tcp port=5190, appl_name=junos-aol, service type=36, alg id=0, timeout=1800
tcp port=5191, appl_name=junos-aol, service type=36, alg id=0, timeout=1800
tcp port=5192, appl_name=junos-aol, service type=36, alg id=0, timeout=1800
tcp port=5193, appl_name=junos-aol, service type=36, alg id=0, timeout=1800
tcp port=5800, appl_name=junos-vnc, service type=40, alg id=0, timeout=1800
tcp port=6000, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6001, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6002, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6003, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6004, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6005, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6006, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6007, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6008, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6009, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6010, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6011, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6012, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6013, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6014, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6015, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6016, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

参考：プリディファインドアプリケーションのタイムアウト値 – TCP 3/4

```
tcp port=6017, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6018, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6019, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6020, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6021, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6022, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6023, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6024, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6025, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6026, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6027, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6028, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6029, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6030, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6031, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6032, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6033, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6034, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6035, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6036, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6037, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6038, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6039, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6040, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6041, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6042, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6043, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6044, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6045, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6046, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6047, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6048, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6049, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6050, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6051, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6052, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6053, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6054, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

参考：プリディファインドアプリケーションのタイムアウト値 – TCP 4/4

```
tcp port=6055, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6056, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6057, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6058, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6059, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6060, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6061, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6062, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6063, appl_name=junos-x-windows, service type=0, alg id=0, timeout=1800
tcp port=6660, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6661, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6662, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6663, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6664, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6665, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6666, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6667, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6668, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=6669, appl_name=junos-irc, service type=0, alg id=0, timeout=1800
tcp port=7001, appl_name=junos-http-ext, service type=66, alg id=0, timeout=1800
tcp port=15397, appl_name=junos-ns-global-pro, service type=0, alg id=0,
timeout=1800
```


Copyright © 2010 Juniper Networks, Inc.

参考：プリディファインドアプリケーションのタイムアウト値 – UDP 1/2

```
udp port=0, appl_name=junos-udp-any, service type=0, alg id=0, timeout=60
udp port=7, appl_name=junos-echo, service type=0, alg id=0, timeout=60
udp port=9, appl_name=junos-discard, service type=19, alg id=0, timeout=60
udp port=19, appl_name=junos-chargen, service type=18, alg id=0, timeout=60
udp port=53, appl_name=junos-dns-udp, service type=16, alg id=16, timeout=60
udp port=67, appl_name=junos-dhcp-server, service type=28, alg id=0, timeout=60
udp port=68, appl_name=junos-dhcp-client, service type=28, alg id=0, timeout=60
udp port=69, appl_name=junos-tftp, service type=29, alg id=29, timeout=60
udp port=111, appl_name=junos-sun-rpc-udp, service type=5, alg id=5, timeout=60
udp port=123, appl_name=junos-ntp, service type=44, alg id=0, timeout=60
udp port=135, appl_name=junos-ms-rpc-udp, service type=55, alg id=55, timeout=60
udp port=137, appl_name=junos-nbname, service type=48, alg id=0, timeout=60
udp port=138, appl_name=junos-nbds, service type=50, alg id=0, timeout=60
udp port=500, appl_name=junos-ike, service type=54, alg id=0, timeout=60
udp port=512, appl_name=junos-biff, service type=0, alg id=0, timeout=60
udp port=513, appl_name=junos-who, service type=0, alg id=0, timeout=60
udp port=514, appl_name=junos-syslog, service type=23, alg id=0, timeout=60
udp port=517, appl_name=junos-talk, service type=65, alg id=65, timeout=60
udp port=518, appl_name=junos-ntalk, service type=65, alg id=65, timeout=60
udp port=520, appl_name=junos-rip, service type=0, alg id=0, timeout=60
udp port=540, appl_name=junos-uucp, service type=0, alg id=0, timeout=60
udp port=646, appl_name=junos-ldp-udp, service type=0, alg id=0, timeout=60
udp port=1434, appl_name=junos-sql-monitor, service type=57, alg id=0, timeout=60
udp port=1701, appl_name=junos-l2tp, service type=0, alg id=0, timeout=60
udp port=1719, appl_name=junos-h323, service type=61, alg id=61, timeout=60
udp port=1812, appl_name=junos-radius, service type=51, alg id=0, timeout=60
udp port=1813, appl_name=junos-radacct, service type=51, alg id=0, timeout=60
udp port=2049, appl_name=junos-nfsd-udp, service type=43, alg id=0, timeout=60
udp port=2123, appl_name=junos-gtp, service type=74, alg id=0, timeout=60
udp port=2427, appl_name=junos-mgcp-ua, service type=72, alg id=72, timeout=7200
udp port=2727, appl_name=junos-mgcp-ca, service type=73, alg id=73, timeout=7200
udp port=3478, appl_name=junos-stun, service type=0, alg id=0, timeout=60
udp port=3479, appl_name=junos-stun, service type=0, alg id=0, timeout=60
udp port=4500, appl_name=junos-ike-nat, service type=54, alg id=0, timeout=60
udp port=5060, appl_name=junos-sip, service type=63, alg id=63, timeout=60
udp port=5632, appl_name=junos-pc-anywhere, service type=0, alg id=0, timeout=60
udp port=6346, appl_name=junos-gnutella, service type=42, alg id=0, timeout=60
udp port=6347, appl_name=junos-gnutella, service type=42, alg id=0, timeout=60
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

参考：プリディファインドアプリケーションのタイムアウト値 – UDP 2/2

```
udp port=7000, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7001, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7002, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7003, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7004, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7005, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7006, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7007, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7008, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7009, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
udp port=7010, appl_name=junos-vdo-live, service type=0, alg id=0, timeout=60
```


Copyright © 2010 Juniper Networks, Inc.

カスタムアプリケーションの登録（オプション）

独自システムのトラフィックを制御したい場合など、カスタムアプリケーションを作成する事が出来ます。また、この時に合わせて、ALGをカスタムアプリケーションで動作させるか指定出来ます。

- Application Protocol
  - DNS,FTP,IGNORE,MGCP-CA,MGCP-UA,PPTP, Q931,RAS,REALAUDIO,RSH,RTSP,SCCP,SIP, SQLNET-V2,TALK,TFTP
  - ‘ignore’ は、ALGを利用しない場合に設定します。
- Source and destination ports
- icmp-type, icmp-code
- IP protocol
- rpc-program-number
- uuid

タイムアウト値は 4-86400 秒の間で設定可能です。

また、事前定義及びカスタムで作成したApplicationをグループ化することも可能です。

Copyright © 2010 Juniper Networks, Inc.

APPLICATION LAYER GATEWAY (ALG)

アプリケーションによっては、適切に通信を制御する為に、L3/L4ヘッダのみならずアプリケーションプロトコルの中身を監視または制御する必要があります。本目的の為に、以下の様な場合に、ALGが利用されます。

- 一つの通信フロー内の制御プロトコルによって、新たに別の通信フローを作成するアプリケーション 。(FTP、SQL等)
- 強固なセキュリティの為に、アプリケーションペイロードを監視する必要がある場合 。(DNS等)
- より上位のセキュリティ機能のために、アプリケーションペイロードを監視する必要がある場合。(http等)
- 同一のポート上で異なる通信フローを区別する必要がある場合。(ESP/NAT等)
- ブランチSRXのJunos10.2時点でサポートされるALGは下記の通りです。
  - DNS、FTP、H.323、MGCP、MS-RPC、PPTP、RSH、RTSP、SIP、SCCP、SUN-RPC、TFTP、Talk ALG、SQL
- ハイエンドSRXで対応しているALGは、ブランチSRXとは異なるのでリリース毎に確認が必要です。

ALGを無効にするには:

- 'set security alg algname disable'で指定ALGがプラットフォーム全体で無効となります。

Copyright © 2010 Juniper Networks, Inc.

カスタムアプリケーション設定例

```
applications {
    application ftp-custom1 {
        application-protocol ftp;
        protocol tcp;
        destination-port 8021;
        inactivity-timeout 3600;
    }
    application ftp-custom2 {
        application-protocol ignore;
        protocol tcp;
        destination-port 9021;
    }
}
```

← Custom Application

← 該当サービスにALGを指定しない Custom Application

Copyright © 2010 Juniper Networks, Inc.

ポリシーの記述

セキュリティポリシー構成要素を用いて、実際のセキュリティポリシーを記述します。

セキュリティポリシーは、ソースと宛先’zone’の指定とポリシー名の設定に加えて、条件に合致する‘match’クライテリア部分と、条件に合致したセッションに対して実行するアクションとなる’then’の部分に分かれています。

- ‘match’クライテリア
  - IPアドレス：source-address, destination-address
  - ポート番号：　application
  - ポリシーの特定時間スケジュールプロファイル指定：Scheduler-name（オプション）
- ‘then’アクション
  - 該当セッション通信トラフィック転送の許可 or 拒否
  - 該当ポリシーがマッチした時点での付随的なアクションの指定

ポリシーは設定の上から順番に評価され、条件にマッチしたアクションが一度のみ実行され、以後のポリシーは評価されません。この為、ポリシーの順番に留意する必要があります。

- ポリシーの順番は、”insert” コマンドにて変更可能です。

Copyright © 2010 Juniper Networks, Inc.

セキュリティポリシー アクションの指定

‘then’ アクション後に指定

- Permit：許可
- Deny：破棄 (無応答、エラーコード返さず）
- Reject：拒否 (tcp-rst または ICMP port unreachable messageエラーコードを明示的に返す）
- Log：ログの取得
- Count：該当ポリシーのパケット数、バイト数を取得

明示的にpolicyを指定しない場合はデフォルトポリシーに指定されているアクションが有効となります。

- デフォルトポリシーは、一番最後に記述されているポリシーとなります。
- デフォルトアクションは，denyとなっていますが，設定によりpermitに変更する事も可能です。
  set security policies default-policy deny-all/permit-all

Copyright © 2010 Juniper Networks, Inc.

セキュリティポリシー設定例

```
# show security policies
from-zone trust to-zone untrust {
policy reject_juniper {
        match {
            source-address any;
            destination-address www.juniper.net
            application any;
        }
        then {
            reject;
            log {
                session-init;
            }
            count {
                alarm per-second-threshold 1;
            }
        }
    }
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
            count {
                alarm per-second-threshold 1;
            }
        }
    }
}
```


Copyright © 2010 Juniper Networks, Inc.

SECURITY LOGGING

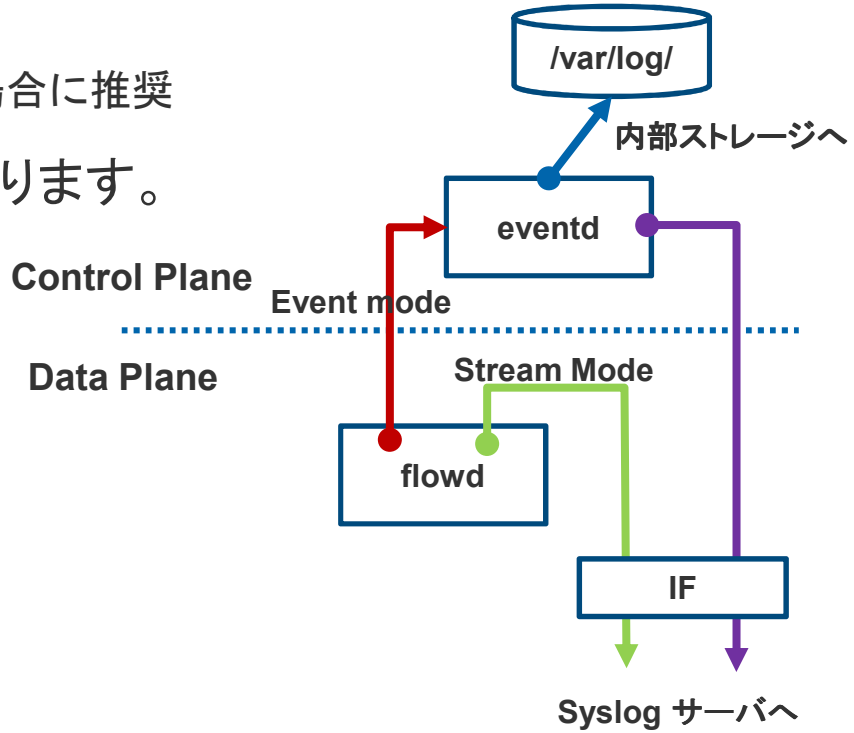
JUNOSのシステムにて利用される通常のシステムログとは別に、トラフィックログ（セキュリティログ）を収集する事が出来ます。

トラフィックログは、二つのフォーマットがあります。

- 通常のsyslog（RFC3164）
- Structured Syslog
  - より詳細なセキュリティ情報を収集したい場合に推奨

トラフィックログには二つの収集方法があります。

- Stream Mode
  - ディフォルト
  - 通常の環境では推奨のモード。
- Event Mode
  - 最大1500 events/sec の制約あり。



Copyright © 2010 Juniper Networks, Inc. www.juniper.net

Security Logging Event-mode 設定例

```
# show system syslog
archive size 100k files 3;
user * {
    any emergency;
}
host 172.27.67.102 {
    any any;
    match RT_FLOW;
}
file messages {
    any critical;
    authorization info;
}
file interactive-commands {
    interactive-commands error;
}
file traffic_log {
    any any;
    match RT_FLOW;
    structured-data;
}
file idp_log {
    match IDP_ATTACK;
    structured-data {
        brief;
    }
}

# show security log
mode event;
event-rate 100;
format sd-syslog;
```

Traffic Logのメッセージは“RT_FLOW”にマッチする事を利用

通常のシステム関連ログ設定

Traffic Logのメッセージは“RT_FLOW”にマッチする事を利用して、別ファイルへ保存
Structured syslogフォーマットを選択

IDP関連ログは”IDP_ATTACK”にマッチ

Event Modeを指定
レートは1500以下
Structured syslogフォーマットを選択

Copyright © 2010 Juniper Networks, Inc.

Security Logging Event-mode / structured syslog 出力例

```
# run show log traffic_log
Oct 17 08:00:02  newsyslog[94428]: logfile turned over due to size>100K
<14>1 2010-10-17T08:24:49.426Z - RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.41 reason="unset" source-address="192.168.1.3" source-
port="1504" destination-address="60.254.131.202" destination-port="80"
service-name="junos-http" nat-source-address="172.27.67.101" nat-source-
port="13786" nat-destination-address="60.254.131.202" nat-destination-
port="80" src-nat-rule-name="source-nat-rule" dst-nat-rule-name="None"
protocol-id="6" policy-name="trust-to-untrust" source-zone-name="trust"
destination-zone-name="untrust" session-id-32="19697" packets-from-
client="91" bytes-from-client="6336" packets-from-server="148" bytes-from-
server="201839" elapsed-time="0"] session closed unset: 192.168.1.3/1504-
>60.254.131.202/80 junos-http 172.27.67.101/13786->60.254.131.202/80
source-nat-rule None 6 trust-to-untrust trust untrust 19697 91(6336)
148(201839) 0
<14>1 2010-10-17T12:54:57.428Z - RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.41 reason="unset" source-address="192.168.1.3" source-
port="1040" destination-address="172.27.0.10" destination-port="53"
service-name="junos-dns-udp" nat-source-address="172.27.67.101" nat-
source-port="56381" nat-destination-address="172.27.0.10" nat-destination-
port="53" src-nat-rule-name="source-nat-rule" dst-nat-rule-name="None"
protocol-id="17" policy-name="trust-to-untrust" source-zone-name="trust"
destination-zone-name="untrust" session-id-32="23772" packets-from-
client="1" bytes-from-client="72" packets-from-server="1" bytes-from-
server="256" elapsed-time="0"] session closed unset: 192.168.1.3/1040-
>172.27.0.10/53 junos-dns-udp 172.27.67.101/56381->172.27.0.10/53 source-
nat-rule None 17 trust-to-untrust trust untrust 23772 1(72) 1(256) 0
```

Attribute名=“Value” のフォーマット

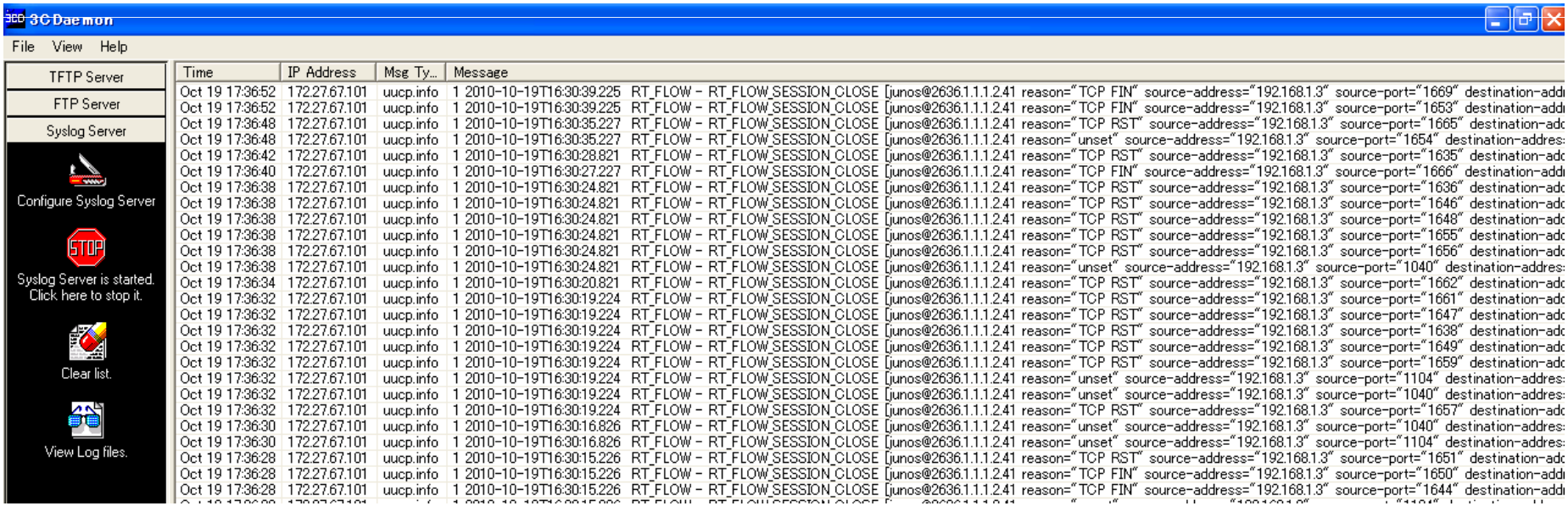
Copyright © 2010 Juniper Networks, Inc.

Security Logging Stream-mode 設定例と出力例

```
# show security log
mode stream;
source-address 172.27.67.101;
stream traffic_log {
    format sd-syslog;
    host {
        172.27.1.177;
    }
}
```

Stream mode を指定
ソースアドレスとsyslogサーバアドレスの指定
Structured syslogフォーマットを選択

Stream modeはREを通らないため、system配下への追加設定は無し



Copyright © 2010 Juniper Networks, Inc. www.juniper.net

Policy Counters

```
# run show security policies detail
Default policy: deny-all
Policy: trust-to-untrust, action-type: permit, State: enabled, Index: 4,
Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4: 0.0.0.0/0
    any-ipv6: ::/0
  Destination addresses:
    any-ipv4: 0.0.0.0/0
    any-ipv6: ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Session log: at-close
  Policy statistics:
    Input  bytes     :          19675258                0 bps
    Output bytes     :          19619954                0 bps
    Input  packets   :             27347                0 pps
    Output packets   :             26869                0 pps
    Session rate     :               804                0 sps
    Active sessions  :                 0
    Session deletions:               804
    Policy lookups   :               804
```

増加カウンタ

秒間レートカウンタ

```
# run clear security policies statistics
```

← ポリシーカウントのクリア

Copyright © 2010 Juniper Networks, Inc.

ポリシー確認コマンド

```
# run show security policies policy-name trust-to-untrust
From zone: trust, To zone: untrust
  Policy: trust-to-untrust, State: enabled, Index: 4, Scope Policy: 0,
Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit, log, count
```


Copyright © 2010 Juniper Networks, Inc.

基本的なFlow/Session挙動の変更

SRXは、以下の5-tupple情報によりステートフルインインスペクションを実行しています。

- Source IP / Port
- Destination IP / Port
- Protocol Number

デフォルトにて、通常的な利用に問題無いように事前設定が行われていますが、基本的なflow/sessionの動作挙動を変更する事も出来ます。

- set security flow …
- set security zones security-zone <zone-name> tcp-rst

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

基本的なフロー挙動の設定

```
lab# set security flow ?
Possible completions:
> aging                  Aging configuration
  allow-dns-reply        Allow unmatched incoming DNS reply packet
+ apply-groups           Groups from which to inherit configuration data
+ apply-groups-except    Don't inherit configuration data from these groups
  route-change-timeout   Timeout value for route change to nonexistent route
(seconds)
  syn-flood-protection-mode  TCP SYN flood protection mode
> tcp-mss                TCP maximum segment size configuration
> tcp-session            Transmission Control Protocol session configuration
> traceoptions           Trace options for flow services
```

通常は、特に変更することなくディフォルト値で問題有りません。

Copyright © 2010 Juniper Networks, Inc.

基本的なTCPフロー挙動の設定

```
lab# set security flow tcp-session ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except   Don't inherit configuration data from these groups
  no-sequence-check     Disable sequence-number checking
  no-syn-check          Disable creation-time SYN-flag check
  no-syn-check-in-tunnel  Disable creation-time SYN-flag check for tunnel
packets
  rst-invalidate-session  Immediately end session on receipt of reset
(RST) segment
  rst-sequence-check    Check sequence number in reset (RST) segment
  strict-syn-check      Enable strict syn check
  tcp-initial-timeout   Timeout for TCP session when initialization fails
(20..300 seconds)
[edit]
```

通常は、特に変更することなくディフォルト値で問題有りません。

Copyright © 2010 Juniper Networks, Inc.

セッションにマッチしないTCPパケットに対する挙動設定

```
lab# set security zones security-zone untrust ?
Possible completions:
  <[Enter]>             Execute this command
> address-book          Address book entries
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except   Don't inherit configuration data from these groups
> host-inbound-traffic   Allowed system services & protocols
> interfaces            Interfaces that are part of this zone
  screen                Name of ids option object applied to the zone
  tcp-rst               Send RST for TCP SYN packet not matching session
  |                     Pipe through a command
[edit]
```

ゾーン単位で、セッションマッチしないTCPセッションに対してRST応答の有無を指定

Copyright © 2010 Juniper Networks, Inc.

通信確認コマンド

```
lab> show security flow session ?
Possible completions:
  <[Enter]>             Execute this command
  application           Application protocol name
  brief                 Show brief output (default)
  destination-port      Destination port (1..65535)
  destination-prefix    Destination IP prefix or address
  extensive             Show detailed output
  family                Show session by family
  idp                   Show idp sessions
  interface             Name of incoming or outgoing interface
  nat                   Show sessions with network address translation
  protocol              IP protocol number
  resource-manager      Show sessions with resource manager
  session-identifier    Show session with specified session identifier
  source-port           Source port (1..65535)
  source-prefix         Source IP prefix or address
  summary               Show output summary
  tunnel                Show tunnel sessions
  |                     Pipe through a command
```

大量のセッションがあるときに特定のセッション情報を指定

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

通信確認コマンド

```
lab> show security flow session summary
Unicast-sessions: 28
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 29
  Valid sessions: 28
  Pending sessions: 0
  Invalidated sessions: 1
  Sessions in other states: 0
Maximum-sessions: 16384
```

セッションの全体数の確認

Copyright © 2010 Juniper Networks, Inc.

通信確認コマンド

```
lab> show security flow session
Session ID: 6352, Policy name: self-traffic-policy/1, Timeout: 1800, Valid
  In: 172.27.3.149/2462 --> 172.27.67.101/23;tcp, If: fe-0/0/0.0, Pkts: 2156,
Bytes: 87809
  Out: 172.27.67.101/23 --> 172.27.3.149/2462;tcp, If: .local..0, Pkts: 1478,
Bytes: 140513

Session ID: 6565, Policy name: trust-to-untrust/4, Timeout: 1788, Valid
  In: 192.168.1.254/2330 --> 207.46.73.60/80;tcp, If: vlan.0, Pkts: 17, Bytes:
2216
  Out: 207.46.73.60/80 --> 172.27.67.101/18983;tcp, If: fe-0/0/0.0, Pkts: 19,
Bytes: 23973

Session ID: 6991, Policy name: trust-to-untrust/4, Timeout: 1774, Valid
  In: 192.168.1.254/2298 --> 64.233.183.138/80;tcp, If: vlan.0, Pkts: 10, Bytes:
3102
  Out: 64.233.183.138/80 --> 172.27.67.101/6412;tcp, If: fe-0/0/0.0, Pkts: 7,
Bytes: 1212

Session ID: 6998, Policy name: self-traffic-policy/1, Timeout: 4, Valid
  In: 172.27.67.101/123 --> 210.173.160.87/123;udp, If: .local..0, Pkts: 1, Bytes:
76
  Out: 210.173.160.87/123 --> 172.27.67.101/123;udp, If: fe-0/0/0.0, Pkts: 1,
Bytes: 76

Session ID: 6999, Policy name: self-traffic-policy/1, Timeout: 10, Valid
  In: 172.27.67.101/123 --> 210.173.160.57/123;udp, If: .local..0, Pkts: 1, Bytes:
76
  Out: 210.173.160.57/123 --> 172.27.67.101/123;udp, If: fe-0/0/0.0, Pkts: 1,
Bytes: 76
```

In: セッション開始方向半二重通信
Out: セッション受け側半二重通信

セッションID

ソースIP/Port

宛先IP/Port

タイムアウト値（秒）

Copyright © 2010 Juniper Networks, Inc.

通信確認コマンド

```
lab> show security flow session session-identifier 10481
Session ID: 10481, Status: Normal
Flag: 0x0
Policy name: trust-to-untrust/4
Source NAT pool: interface, Application: junos-http/6
Maximum timeout: 1800, Current timeout: 1762
Session State: Valid
Start time: 356796, Duration: 40
   In: 192.168.1.254/2603 --> 63.150.131.174/80;tcp,
    Interface: vlan.0,
    Session token: 0x6, Flag: 0x0x21
    Route: 0xa0010, Gateway: 192.168.1.254, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 56, Bytes: 2669
   Out: 63.150.131.174/80 --> 172.27.67.101/59196;tcp,
    Interface: fe-0/0/0.0,
    Session token: 0x7, Flag: 0x0x20
    Route: 0x70010, Gateway: 172.27.66.1, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 104, Bytes: 150773
Total sessions: 1
```


Copyright © 2010 Juniper Networks, Inc.

SCREEN機能

Screen 機能は、L3/L4の基本的な攻撃防御機能を提供します。

IDPモジュールは用いない独立した機能となり、非常に高速に動作します。

- ハイエンドSRXでは、NPC/SPU上に実現
- ブランチSRXでは、SPU上で処理

Screen機能は、攻撃防御の組（idp-option）を作成し、それをzone毎割り当てる事により設定します。

Copyright © 2010 Juniper Networks, Inc.

Screen機能の設定例 – デフォルトuntrust-screen設定

```
lab# set security screen ids-option untrust-screen ?
Possible completions:
  alarm-without-drop   Do not drop packet, only generate alarm
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> icmp                 Configure ICMP ids options
> ip                   Configure IP layer ids options
> limit-session        Limit sessions
> tcp                  Configure TCP Layer ids options
> udp                  Configure UDP layer ids options
[edit]
lab# set security screen ids-option untrust-screen tcp ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  fin-no-ack           Enable Fin bit with no ACK bit ids option
  land                 Enable land attack ids option
> port-scan            Configure port scan ids option
> syn-ack-ack-proxy    Enable syn-ack-ack proxy ids option
  syn-fin              Enable SYN and FIN bits set attack ids option
> syn-flood            Enable SYN flood ids option
  syn-frag             Enable SYN fragment ids option
  tcp-no-flag          Enable TCP packet without flag ids option
> tcp-sweep            Configure TCP sweep ids option
  winnuke              Enable winnuke attack ids option
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

Screen機能の確認例

```
lab> show security screen statistics zone untrust
Screen statistics:

IDS attack type                                Statistics
  ICMP flood                                   5
  UDP flood                                    21
  TCP winnuke                                  0
  TCP port scan                                0
  ICMP address sweep                           0
  TCP sweep                                    12
  UDP sweep                                    15
  IP tear drop                                 0
  TCP SYN flood                                0
  IP spoofing                                  0
  ICMP ping of death                           0
  IP source route option                       0
  TCP land attack                              0
  TCP SYN fragment                             0
  TCP no flag                                  0
  IP unknown protocol                          154
  IP bad options                               0
  IP record route option                       0
  IP timestamp option                          0
  IP security option                           0
  IP loose source route option                 0
  IP strict source route option                0
  IP stream option                             0
  ICMP fragment                                0
  ICMP large packet                            210
  TCP SYN FIN                                  0
  TCP FIN no ACK                               0
  Source session limit                         0
  TCP SYN-ACK-ACK proxy                        0
  IP block fragment                            0
  Destination session limit                    0
```

該当Screenにヒットしたカウント値

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

FW処理関連トラブルシューティング

パケットが正常に転送されない場合、以下例の理由が考えられます

- SRXにパケットが到達しているか？
- flowの設定が、意図したものになっているか？
- Screen機能によりパケットがブロックされていないか？
- パケットの宛先は、ファイアウォール自身か？
- 非対称ルートになっていないか？
- 既存セッションのパケットか？
- ALGによりブロックされていないか？
- パケットは正しいインタフェース/ゾーンから到達しているか？
- 適切なルート/L2フォーワードパスが選択されているか？
- 正しいポリシーが選択されているか？
- ポリシーベースのNATが正しく適用されているか？

Copyright © 2010 Juniper Networks, Inc.

FW処理関連トラブルシューティング切り分け手段

該当セッションが存在しているかどうかの確認

- “show security flow session”により確認

パケット到達性の確認

- “monitor interface traffic” によるIFリアルタイムカウンタの確認

RE処理イベントの確認

- messagesファイル内容の確認
- “monitor traffic …” コマンドによるプロトコルイベント確認

FW処理によるトラフィックドロップの確認

- ポリシーカウンタの確認
- トラフィックログ（セキュリティログ）出力内容の確認
- flow traceoptionによるデバッグ出力内容の確認

実パケット内容の確認

- パケットキャプチャによる、実パケット内容の確認

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

FLOW/SESSION デバッグの取得（TRACEOPTION設定）

‘set security flow traceoption …’にて、フロー/セッションのデバッグを取得する事が出来ます。(ScreenOSでの’debug flow …’に相当）

Set security flow traceoptions flag packet-drops

- ドロップされたパケットのデバッグログ取得指定します。
- 意図しないトラフィックがSRXにて落とされている可能性がある場合、まずは本オプションを指定して動作を切り分けします。

set security flow traceoptions flag basic-datapath

- トラフィックフローのデバッグログ取得指定（ScreenOSのdebug flow basicと同じ）

set security flow traceoptions file <file>

- トラフィックフローのデバッグログの保存先指定

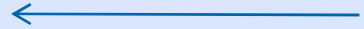
set security flow traceoptions packet-filter <filter名>

- トラフィックフローデバッグのフィルタリング指定

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

デバッグ取得設定

```
lab# set security flow traceoptions flag ?
Possible completions:
  all                  All events
  basic-datapath       Basic packet flow
  packet-drops         Packet drops
[edit]
lab# set security flow traceoptions packet-filter ?
Possible completions:
  <filter-name>        Name of the filter
[edit]
lab# set security flow traceoptions rate-limit ?
Possible completions:
  <rate-limit>         Limit the incoming rate of trace messages
(0..4294967295)
```

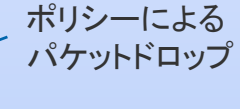


通常のデバッグでは
packet dropsを指定

Copyright © 2010 Juniper Networks, Inc.

デバッグ内容確認

```
lab# set security flow traceoptions flag packet-drops
lab# set security flow traceoptions file flow-trace

[edit]
lab# commit
commit complete

[edit]
lab# run show log flow_debug.txt | last


Oct 19 18:43:21 18:43:21.621877:CID-0:RT:  vlan.100:172.27.1.177/3807-
>172.27.67.101/23, tcp, flag 10

Oct 19 18:43:21 18:43:21.771920:CID-0:RT:  vlan.0:192.168.1.3-
>172.27.1.177, icmp, (8/0)

Oct 19 18:43:21 18:43:21.771920:CID-0:RT:  packet dropped, denied by
policy

Oct 19 18:43:21 18:43:21.771920:CID-0:RT:  packet dropped,  policy deny.

Oct 19 18:43:22 18:43:22.674546:CID-0:RT:  vlan.100:172.27.1.177/3807-
>172.27.67.101/23, tcp, flag 18

Oct 19 18:43:22 18:43:22.677320:CID-0:RT:  .local..0:172.27.67.101/23-
>172.27.1.177/3807, tcp, flag 18

Oct 19 18:43:23 18:43:22.825169:CID-0:RT:  vlan.100:172.27.1.177/3807-
>172.27.67.101/23, tcp, flag 10
```



Copyright © 2010 Juniper Networks, Inc.


everywhere