Understanding Migrated Configurations and Events

With very few exceptions, Version 5.2 can perform the same level of intrusion protection, network awareness, and event analysis as Version 4.10.3, and adds many additional features and capabilities. The migration scripts that Cisco provides are designed to allow you to reimage sensors and transfer vital configurations and events from either a Version 4.10.3 Defense Center or a standalone 3D Sensor to a Version 5.2 Defense Center.

In general, you can migrate the following configurations and events:

- intrusion policies, variables, and local rules
- PEP rules from applied PEP policies
- settings from applied RNA detection policies, including networks to monitor
- RNA-related settings in the applied system policy and NetFlow devices specified in the system settings
- compliance policies, compliance rules, and traffic profiles
- 3D Sensor-based RUA configurations
- intrusion and audit events
- interface configurations, when you use the sensor migration script

Note, however, that due to the updated way in which Version 5.2 handles and analyzes traffic, you may not be able to successfully or cleanly migrate specific settings within these configurations.

Any configuration not listed above is **not** migrated, including (but not limited to) unapplied policies; users, preferences, and roles, including LDAP configurations; compliance responses and white lists; RNA detectors and custom fingerprints; health policies; custom workflows, tables, and searches; reports; dashboards; other types of events; and so on. Note that interface configurations are not copied if you do not use the sensor migration script.

This chapter explains which Version 4.10.3 configurations are migrated, including exceptions within those configurations, and how you can expect the migrated settings to appear in Version 5.2.

Note This chapter summarizes basic concepts. For detailed information on Version 5.2 features, see the Version 5.2 *Sourcefire 3D System User Guide*.

For more information, see:

- Understanding the New Access Control Policy, page 5-2

Understanding the New Access Control Policy

Access control is a new policy-based feature that allows you to specify, inspect, and log the traffic that can traverse your network. An *access control policy*, which you apply to one or more *target devices*, determines how the system handles traffic on your network.

Along with many added features for Version 5.2, access control policies can perform the following analysis and traffic handling that you could also perform in Version 4.10.3:

- Using access control rules with access control policies, you can duplicate the functionality of most PEP rules to trust (sometimes called *fast path*) specific traffic.
- Using access control rules, you can invoke intrusion policies to analyze, and optionally block, traffic based on intrusions and exploits.
- Access control policies define the traffic that you permit and, therefore, the traffic you can monitor with the discovery feature (previously called *RNA*).

The migration process creates a new access control policy on the Version 5.2 Defense Center every time you import a configuration package from a either a Version 4.10.3 3D Sensor or Defense Center.

Note that if the import script cannot build an access control policy using the configurations in an exported Version 4.10.3 package (for example, because the package does not contain the necessary configurations), the script creates a new access control policy with no rules and using Version 5.2 defaults.

After you finish the import process and modify the new access control policy to accommodate any configurations not migrated, you can apply the policy; see Applying Network Discovery and Access Control Policies, page 4-38.

Target Devices

An access control policy target device, or *target*, is simply a device where you apply the policy. When you add devices to the Version 5.2 Defense Center after you complete the configuration import, you specify the access control policies to apply to those devices. The Defense Center adds the devices as targets for the appropriate policies.

Access Control Rules

Access control rules in an access control policy define how traffic is handled by managed devices. These rules can allow, monitor, inspect, or block traffic based on multiple criteria. They can perform simple IP matching, or create complex scenarios involving different networks, users, applications, ports, and URLs.

The migration process adds rules to the new access control policy based on your Version 4.10.3 PEP rules, applied intrusion policies, and RNA detection policy settings.

Default Action

When you import configurations onto the Defense Center, you name the new access control policy and specify its default action; see Providing Basic Access Control Settings, page 4-15. In Version 5.2, the access control policy's *default action* specifies how the system handles traffic that does not meet the conditions of any access control rule in an access control policy.

The script prompts you to select an intrusion policy to associate with the default action, and using it to inspect all default-action traffic. You can choose any intrusion policy that exists on the Version 5.2 Defense Center, or you can choose one from the configuration package you are importing. The script lists both system-provided and user-created policies. The default is to associate the system-provided Balanced Security and Connectivity intrusion policy with the default action.

You can also create a default action that is **not** associated with an intrusion policy, but that allows all default-action traffic to be inspected by network discovery. This is useful in discovery-only (RNA-only) deployments.

Logging

Connection logging (formerly flow data logging) is now configured as part of access control, rather than as a part of network discovery. The migration process uses the flow data collection preferences in your Version 4.10.3 RNA detection policies to set connection logging preferences for each access control rule and the access control policy default action. However, this split complicates the migration of Version 4.10.3 port exclusion preferences. The migration must create multiple access control rules for combinations of intrusion inspection and port exclusions so that you do not log specified traffic.

See the following sections for more information:

- Migrating PEP Rules into Access Control Rules, page 5-3
- Migrating Intrusion Policies and Creating Access Control Rules, page 5-4
- Migrating RNA Settings into Rules and Logging Preferences, page 5-7
- Example Migrated Access Control Rules, page 5-10

Migrating PEP Rules into Access Control Rules

PEP was a feature in Version 4.10.3 that allowed you to create rules to block or send traffic directly through some 3D Sensors with no further inspection.

Note Of the two components of PEP policies in Version 4.10.3 (fast-path rules and PEP rules), only IPv4 and IPv6 PEP rules in applied PEP policies are migrated into access control rules. Version 4.10.3 fast-path rules are **not** migrated; you must configure these rules at the device level after you add devices to your Version 5.2 deployment. For more information, see the *Managing Devices* chapter in the *Version 5.2 Sourcefire 3D System User Guide*.

The migration places PEP-created access control rules at the top of the new access control policy so that they are evaluated first. The migration also prioritizes IPv6 PEP rules over IPv4 PEP rules. Note that only PEP rules in applied, non-deleted policies can be migrated.

The migration converts PEP rules to access control rules as described in the following table.

Table 5-1 PEP Rule Migration

If the PEP Rule action was...	The access control rule action is...	And the PEP rule becomes...
Drop	Block	a single access control rule that blocks the traffic specified by the PEP rule. Blocked traffic is not subject to inspection of any kind.
Drop w/ Reset	Block with reset	a single access control rule that blocks the traffic specified by the PEP rule, and resets the connection. Blocked traffic is not subject to inspection of any kind.
Fast Path (or DE Specific where IPS, RNA, and RUA are all set to Fast Path)	Trust	a single access control rule that trusts the traffic specified by the PEP rule. Trusted traffic is not subject to inspection of any kind.
Analyze (or DE Specific where IPS, RNA, and RUA are all set to Analyze)	Allow	a set of access control rules that ensures all traffic specified by the PEP rule is inspected. The network conditions for these access control rules represent the intersection of the networks in the PEP rule and all other rules in the new access control policy.
DE Specific: • IPS set to Fast Path • RNA and RUA set to Analyze	Allow	a set of access control rules that ensures all traffic specified by the PEP rule is eligible to be monitored by discovery, but is not inspected by an intrusion policy. The network conditions for these access control rules represent the intersection of the networks in the PEP rule and all other rules in the new access control policy.
DE Specific: • IPS set to Analyze • RNA or RUA set to Fast Path	n/a	Because of the way Version 5.2 access control rules handle traffic, you cannot have traffic bypass discovery (RNA or RUA) but still be analyzed by an intrusion policy (IPS). These PEP rules **cannot** be migrated; see Resolving Unsupported RNA and RUA Fast-Path PEP Rules, page 4-12.

Migrating Intrusion Policies and Creating Access Control Rules

The migration transfers all applied Version 4.10.3 intrusion policies and settings into Version 5.2 intrusion policies as-is, with the following exceptions:

- VLAN and network filtering (that is, using an intrusion policy to monitor a specific VLAN or subnetwork) has moved out of the intrusion policy and into the access control rule that invokes the policy.
- Intrusion policies can no longer target detection engines. In Version 5.2, access control rules determine which intrusion policies examine which traffic.
- With Version 5.2, you can no longer explicitly configure IPS detection engine variables.
- You must add service metadata (a new requirement) to all local intrusion rules that inspect traffic on specific ports.
- OPSEC configurations within a Version 4.10.3 intrusion policy are not migrated because Version 5.2 does not support OPSEC configuration.

Note that although it is no longer in the intrusion policy, the migration process converts VLAN and target information into equivalent settings in the access control policy. The migration process can also migrate detection variables at the cost of a proliferation of intrusion policies.

Version 5.2 intrusion policies are named the same as their Version 4.10.3 counterparts. Intrusion policies created to handle custom detection engine variables reference the detection engine, for example:

```
policy_name (copy for variables from 'detection_engine')
```

For more information, see:

- Understanding Access Control Rules That Perform Intrusion Inspection, page 5-5
- Migrating Detection Engine Variables Into Policy Variables, page 5-7
- Adding Service Metadata to Intrusion Rules, page 4-11

Understanding Access Control Rules That Perform Intrusion Inspection

In Version 5.2, access control rules determine which intrusion policies examine which traffic. To migrate this functionality, each Version 4.10.3 intrusion policy-detection engine pair in Version 4.10.3 creates at least one access control rule.

- An **unfiltered** (not restricted by network or VLAN) intrusion policy applied to one detection engine creates **one** access control rule that invokes that intrusion policy.
- A VLAN-or-network **filtered** policy creates **two** rules that invoke that intrusion policy: one rule has a network condition that matches source traffic, the other, destination traffic.

Each access control rule is also restricted by security zone (collection of interfaces), which ensures that the rule's associated intrusion policy monitors only the traffic flowing through certain interfaces.

The following table explains how specific access control rule settings depend on your Version 4.10.3 configurations. All other settings in the created access control rules use Version 5.2 defaults. Note that only filtered policies have network and VLAN conditions.

Table 5-2 Migrated Access Control Rule Settings

Version 4.10.3 Policy Type	Access Control Rule Setting	Details
all	**Action**, which determines how matching traffic is handled and inspected	All access control rules created to perform intrusion inspection must have an action of Allow.
all	**Enabled**, which determines whether the rule is used	Access control rules created by the migration are enabled by default.
all	**Source Zones** (Zone tab), which determines the interfaces whose traffic the rule examines	Restricting access control rules by zone preserves the Version 4.10.3 setting where each intrusion policy was applied to an IPS detection engine, which would monitor the traffic flowing through a specified interface set. For more information, see Understanding How Interface Sets Become Security Zones, page 5-12.
all	**Intrusion Policy** (Inspection table)	All access control rules created to perform intrusion inspection have an associated intrusion policy.
all	enabled **Log at End of Connection** and **Send Connection Events to Defense Center** settings on the Logging tab	The logging settings for an access control rule depend on settings in your Version 4.10.3 RNA detection policies. For more information, see Migrating RNA Settings into Rules and Logging Preferences, page 5-7.

Table 5-2 Migrated Access Control Rule Settings (continued)

Version 4.10.3 Policy Type	Access Control Rule Setting	Details
network-filtered	**Source Networks** or **Destination Networks** (Networks tab)	Access control rules created to inspect traffic with a network-filtered intrusion policy use the deprecated **Policy by VLAN or Network** settings from the Version 4.10.3 intrusion policy to specify source and destination network constraints for the access control rules.
VLAN-filtered	**Selected VLAN Tags** (VLAN Tags tab)	Access control rules created to inspect traffic with a VLAN-filtered intrusion policy use the deprecated **Policy by VLAN or Network** settings from the Version 4.10.3 intrusion policy to specify VLAN constraints for the access control rules.

Access control rules based on intrusion policies use the following naming syntax:

```
policy <non-filtered|<src IP|dst IP|vlan tag#>> on zone
```

where:

- *policy* is the name of the applied policy, or policy copy in the case of custom detection engine variables.
- *IP* is the source or destination network configuration derived from the **Network** field in a Version 4.10.3 network-filtered policy.
- *tag#* is the VLAN tag configuration derived from the **VLAN** field in a Version 4.10.3 VLAN-filtered policy.
- *zone* is the security zone created from the interface set configured on the detection engine where the migrated policy was applied.

Access control rules created by the migration process have long, descriptive names for your convenience. If you edit these rules, you must rename them using no more than 30 characters before you save them. The following table provides example names for different access control rules derived from an intrusion policy named `Mypolicy`.

Table 5-3 Example Access Control Rules Names

Policy Configuration	Access Control Rule Name
non-filtered policy	MyPolicy non-filtered on Myzone
non-filtered policy applied to three detection engines	MyPolicy non-filtered on Myzone-1 MyPolicy non-filtered on Myzone-2 MyPolicy non-filtered on Myzone-3
VLAN-filtered policy with VLAN tags 1, 2, and 3 configured	MyPolicy vlan 1,2,3 on Myzone
network-filtered policy (source rule) with IP addresses 10.1.1.1, 10.1.1.2, and 10.5.0.0/16 configured	MyPolicy src 10.1.1.1, 10.1.1.2, 10.5.0.0/16 on Myzone
network-filtered (policy destination rule) with IP addresses 10.1.1.1, 10.1.1.2, and 10.5.0.0/16 configured	MyPolicy dst 10.1.1.1, 10.1.1.2, 10.5.0.0/16 on Myzone
non-filtered policy applied to detection engine DE-x with custom variables	MyPolicy (copy for variables on ‘DE-x’) non-filtered on Myzone

Table 5-3 Example Access Control Rules Names (continued)

Policy Configuration	Access Control Rule Name
VLAN-filtered policy with VLAN tag 1, applied to detection engine DE-x with custom variables	MyPolicy (copy for variables on 'DE-x') vlan 1 on Myzone
network-filtered policy (source rule) with IP address 10.5.1.2, applied to detection engine DE-x with custom variables	MyPolicy (copy for variables on 'DE-x') src 10.5.1.2 on Myzone

Migrating Detection Engine Variables Into Policy Variables

In the Sourcefire 3D System, a variable is a representation of a port or network value that is commonly used in intrusion rules. Rather than hard-coding these values in multiple rules, you can tailor a rule to accurately reflect your network environment by changing the variable value.

In Version 4.10.3 you could configure custom variables for IPS detection engines, which had priority over intrusion policy-specific variables which, in turn, had priority over system variables. The migration transfers your policy-specific variables to Version 5.2, and also creates a system variable for each migrated policy-specific variable, using the same variable name and a value of `any`.

However, with Version 5.2, you no longer explicitly configure detection engines or detection engine variables. This means that you cannot cleanly migrate a Version 4.10.3 intrusion policy applied to IPS detection engines that use custom variables.

To replicate Version 4.10.3 functionality and migrate custom detection engine variables, the import script can create a copy of the intrusion policy for each active detection engine that used custom variables. These copies use the original intrusion policy as the base policy; each one has different policy-specific variables that correspond to one of the Version 4.10.3 custom variable sets.

Because this can result in a proliferation of intrusion policies, the import script prompts you whether to create the copies. If you decline, the script does not migrate custom detection engine variables and your Version 5.2 configurations will use only the parent intrusion policy.

For Version 4.10.3 IPS detection engines with custom variables but without an intrusion policy applied, the migration converts each custom variable to a system variable using the same variable name and a value of `any`.

Migrating RNA Settings into Rules and Logging Preferences

In Version 4.10.3, you configured host discovery and flow data logging in RNA detection policies. In Version 5.2, logging and monitoring functionality is split: the access control policy governs which connections (flows) are logged on a per-access control rule basis, but the network discovery policy governs discovery.

The migration process uses the flow data logging settings in your applied Version 4.10.3 RNA detection policies to determine how to configure connection logging in the Version 5.2 access control policy, which is done using access control rules.

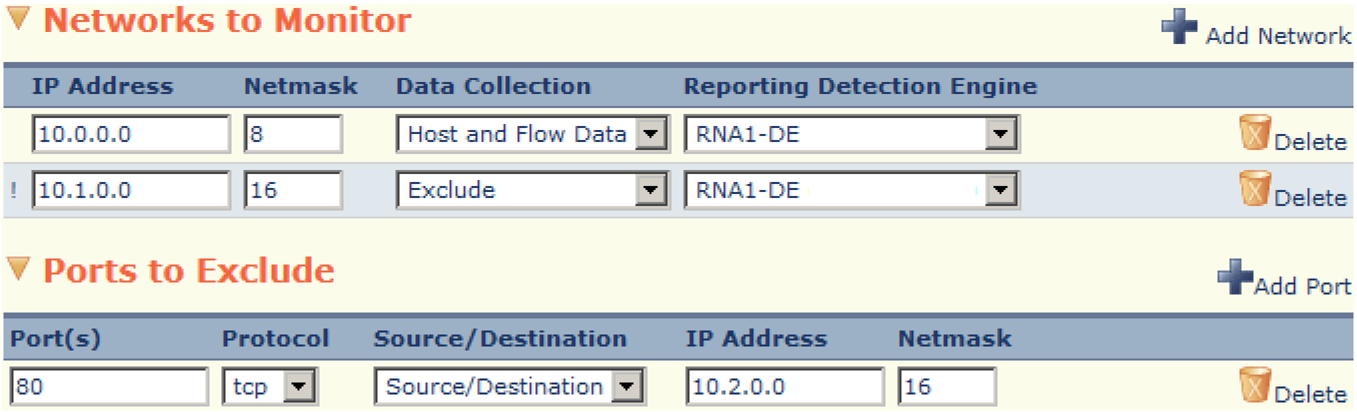
- To exclude traffic to and from a specific port (on one or more hosts) from connection logging while preserving logging and inspection for other hosts, the migration must create **multiple** access control rules for combinations of intrusion inspection and port exclusion preferences.

- To log (or exclude from logging) connections for a particular network, the migration adds **two** access control rules for each network to monitor-detection engine combination in the Version 4.10.3 RNA detection policy, once for source traffic and one for destination traffic. For example, if an RNA detection policy is applied to three different detection engines, the migration adds six access control rules.

Access Control Rule Order

The system places port exclusion-based rules above rules based on networks to monitor or exclude. For example, note the Version 4.10.3 network configurations in the following graphic:

- network to monitor: 10.0.0.0/8
- excluded network: 10.1.0.0/16
- excluded ports: 80 (tcp) on 10.2.0.0/16 in source/destination traffic



Networks to Monitor

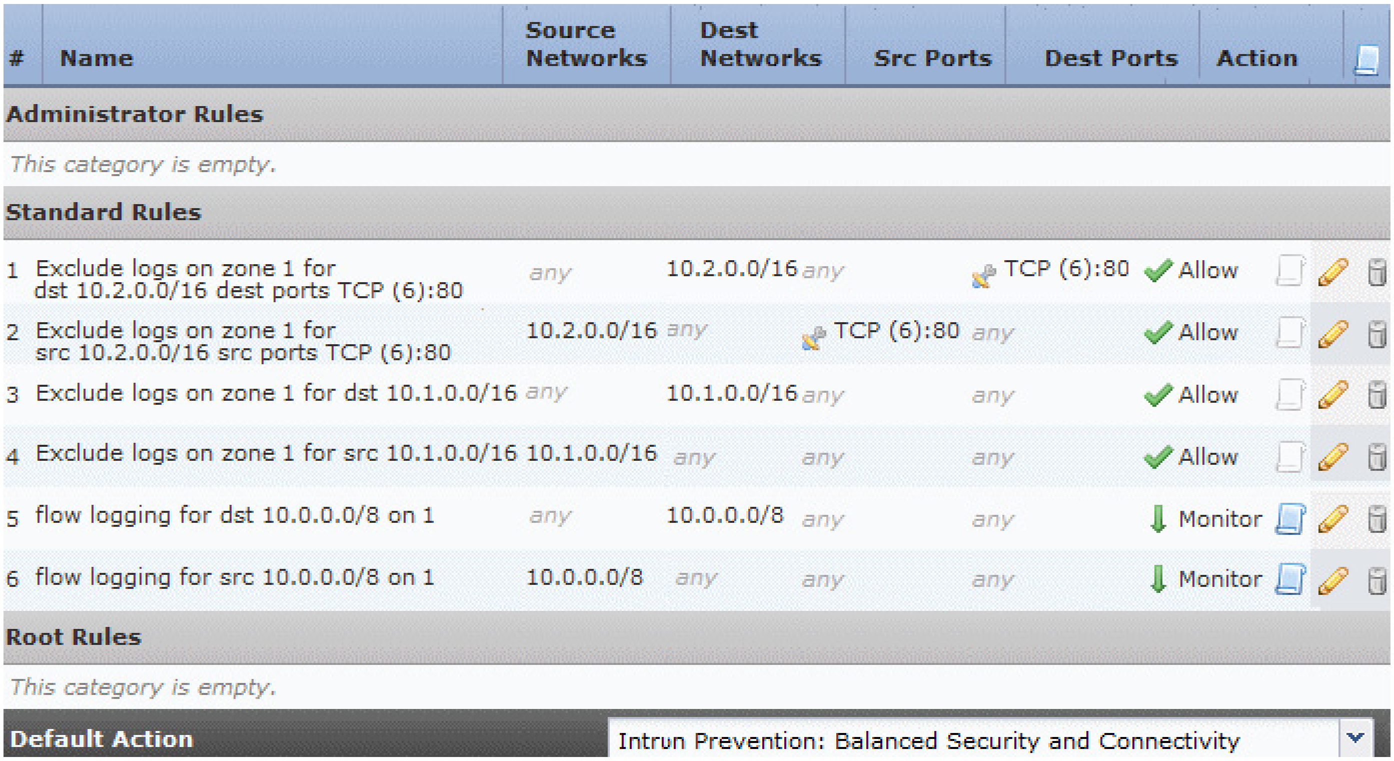
	IP Address	Netmask	Data Collection	Reporting Detection Engine	
	10.0.0.0	8	Host and Flow Data	RNA1-DE	Delete
!	10.1.0.0	16	Exclude	RNA1-DE	Delete

Ports to Exclude

Port(s)	Protocol	Source/Destination	IP Address	Netmask	
80	tcp	Source/Destination	10.2.0.0	16	Delete

372705

The following graphic shows the access control rules for the migrated configurations in the example. Note that, for clarity, not all columns are shown.



#	Name	Source Networks	Dest Networks	Src Ports	Dest Ports	Action
Administrator Rules						
This category is empty.						
Standard Rules						
1	Exclude logs on zone 1 for dst 10.2.0.0/16 dest ports TCP (6):80	any	10.2.0.0/16	any	TCP (6):80	✓ Allow
2	Exclude logs on zone 1 for src 10.2.0.0/16 src ports TCP (6):80	10.2.0.0/16	any	TCP (6):80	any	✓ Allow
3	Exclude logs on zone 1 for dst 10.1.0.0/16	any	10.1.0.0/16	any	any	✓ Allow
4	Exclude logs on zone 1 for src 10.1.0.0/16	10.1.0.0/16	any	any	any	✓ Allow
5	flow logging for dst 10.0.0.0/8 on 1	any	10.0.0.0/8	any	any	↓ Monitor
6	flow logging for src 10.0.0.0/8 on 1	10.0.0.0/8	any	any	any	↓ Monitor
Root Rules						
This category is empty.						
Default Action	Intrun Prevention: Balanced Security and Connectivity					

Note the following configurations in the second graphic:

- Rules 1 and 2 allow traffic for the excluded port 80 on 10.2.0.0/16 to proceed without further processing.
- Rules 3 and 4 allow traffic for the excluded network 10.1.0.0/16 to proceed without further processing.
- Rules 5 and 6 monitor remaining traffic on network 10.0.0.0/8. The logging icon (📄) for these rules indicates that the system logs connections in matching traffic.

The following table describes the configuration of each access control rule created from an applied intrusion policy.

Table 5-4 Migrated Access Control Rule Settings

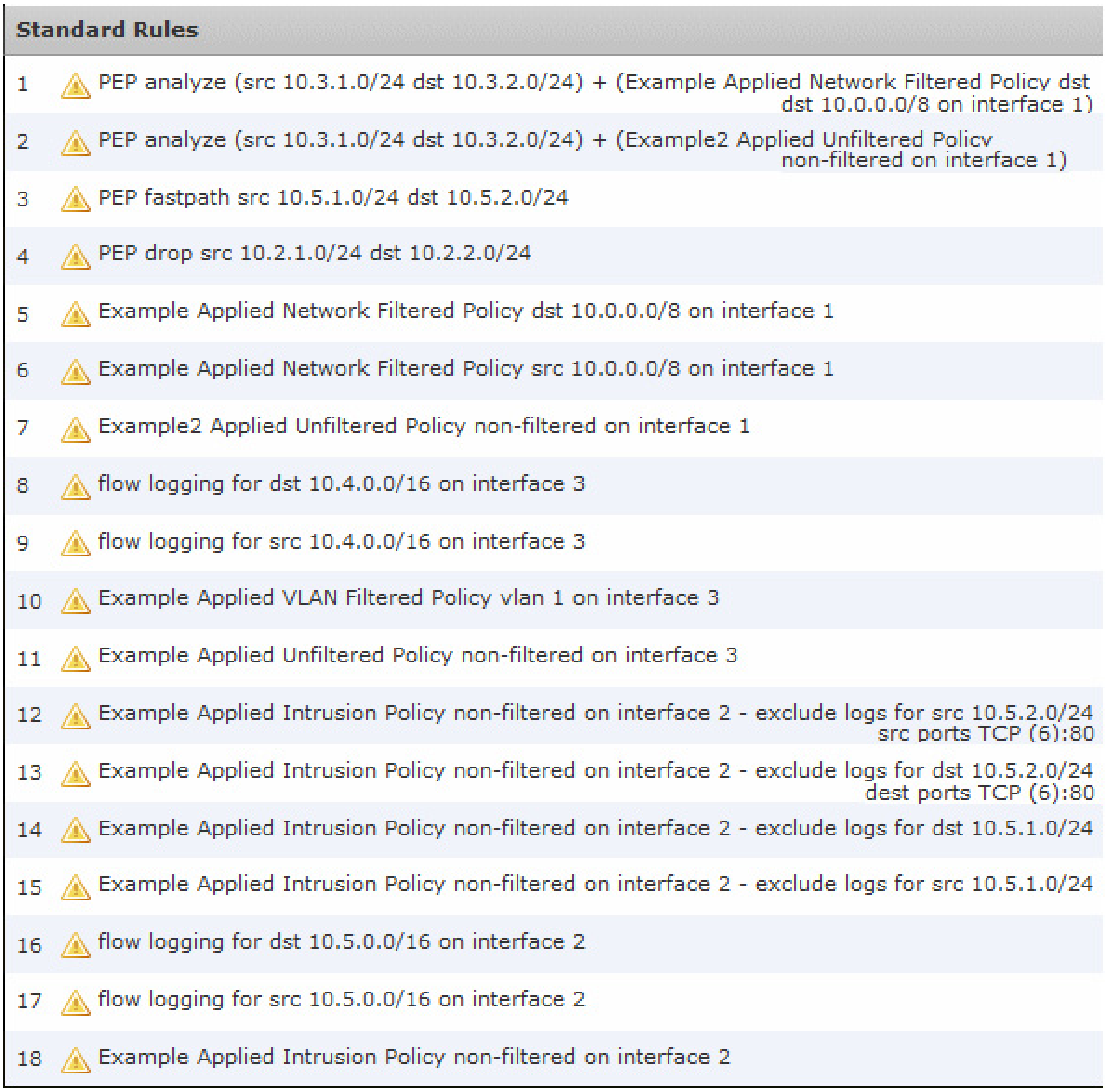
Version 4.10.3 Configuration	Version 5.2 Access Control Rule Setting	Details
a network to monitor	an **Action** of **Monitor** **Source Networks** or **Destination Networks** (Networks tab)	Access control rules created to log connections have an action of **Monitor** to ensure that logging is enabled. This action also allows traffic to match subsequent access control rules. These rules also specify which network they are monitoring.
a network to exclude from monitoring	an **Action** of **Allow**	Access control roles created to allow traffic to pass without logging have an action of **Allow** but disabled logging options. These rules have an associated intrusion policy if your Version 4.10.3 deployment monitored that network with one.

Table 5-4 Migrated Access Control Rule Settings (continued)

Version 4.10.3 Configuration	Version 5.2 Access Control Rule Setting	Details
a port to exclude from monitoring	an **Action** of **Allow** **Selected Destination Ports** or **Selected Source Ports** (Ports tab)	Access control roles created to allow port-based traffic to pass without logging or inspection have an action of **Allow**, but no associated intrusion policy or logging options. These rules also specify which ports and protocols they are excluding.
Reporting Detection Engine for a network	**Zones** (Zones tab)	Restricting logging by zone preserves the Version 4.10.3 setting where each network was monitored by a specific RNA detection engine, which would log the traffic flowing through a specified interface set. For more information, see Understanding How Interface Sets Become Security Zones, page 5-12.
Host and Flow Data collection option for a network	enabled **Log at End of Connection** and **Send Connection Events to Defense Center** settings on the Logging tab	The logging settings for an access control rule depends on settings in your Version 4.10.3 RNA detection policies. For more information, see Migrating RNA Settings into Rules and Logging Preferences, page 5-7.
n/a	**Intrusion Policy** (Inspection table)	All access control rules created to perform intrusion inspection have an associated intrusion policy. Whether an access control rule that logs connections has an associated intrusion policy depends on your Version 4.10.3 intrusion configurations; see Migrating Intrusion Policies and Creating Access Control Rules, page 5-4.
n/a	**Enabled**, which determines whether the rule is used	Access control rules created by the migration are enabled by default.

Example Migrated Access Control Rules

The following graphic includes example access control rules for each type of configuration that populates the access control policy created by the migration.



Standard Rules

1 ⚠ PEP analyze (src 10.3.1.0/24 dst 10.3.2.0/24) + (Example Applied Network Filtered Policy dst dst 10.0.0.0/8 on interface 1)

2 ⚠ PEP analyze (src 10.3.1.0/24 dst 10.3.2.0/24) + (Example2 Applied Unfiltered Policy non-filtered on interface 1)

3 ⚠ PEP fastpath src 10.5.1.0/24 dst 10.5.2.0/24

4 ⚠ PEP drop src 10.2.1.0/24 dst 10.2.2.0/24

5 ⚠ Example Applied Network Filtered Policy dst 10.0.0.0/8 on interface 1

6 ⚠ Example Applied Network Filtered Policy src 10.0.0.0/8 on interface 1

7 ⚠ Example2 Applied Unfiltered Policy non-filtered on interface 1

8 ⚠ flow logging for dst 10.4.0.0/16 on interface 3

9 ⚠ flow logging for src 10.4.0.0/16 on interface 3

10 ⚠ Example Applied VLAN Filtered Policy vlan 1 on interface 3

11 ⚠ Example Applied Unfiltered Policy non-filtered on interface 3

12 ⚠ Example Applied Intrusion Policy non-filtered on interface 2 - exclude logs for src 10.5.2.0/24 src ports TCP (6):80

13 ⚠ Example Applied Intrusion Policy non-filtered on interface 2 - exclude logs for dst 10.5.2.0/24 dest ports TCP (6):80

14 ⚠ Example Applied Intrusion Policy non-filtered on interface 2 - exclude logs for dst 10.5.1.0/24

15 ⚠ Example Applied Intrusion Policy non-filtered on interface 2 - exclude logs for src 10.5.1.0/24

16 ⚠ flow logging for dst 10.5.0.0/16 on interface 2

17 ⚠ flow logging for src 10.5.0.0/16 on interface 2

18 ⚠ Example Applied Intrusion Policy non-filtered on interface 2

The warning (⚠) icons in the graphic indicate that interfaces for the rules are not yet configured.

The following table describes the rules in the graphic.

Table 5-5 Example Access Control Rules

This Rule...	Appears Because the Exported Configurations Included...
1, 2	a PEP rule with the action Analyze, an initiator in the network 10.3.1.0/24, and a responder in the network 10.3.2.0/24; the rule intersects with network 10.0.0.0/8 targeted in the network-filtered policy *Example Applied Network Filtered Policy.* The complexities of the migration, including the presence of rules 3 and 4, make these rules necessary.
3	a PEP rule with the action Fast Path, an initiator in the network 10.5.1.0/24, and a responder in the network 10.5.2.0/24.

Table 5-5 Example Access Control Rules (continued)

This Rule...	Appears Because the Exported Configurations Included...
4	a PEP rule with the action Drop, an initiator in the network 10.2.1.0/24, and a responder in the network 10.2.2.0/24.
5, 6	a network-filtered intrusion policy targeting the network 10.0.0.0/8 and named *Example Applied Network Filtered Policy*; the policy was applied to a detection engine that used an interface that was migrated to a zone named *interface 1*.
7	an unfiltered intrusion policy named *Example2 Applied Unfiltered Intrusion Policy* which; the policy was applied to a detection engine that used an interface that was migrated to a zone named *interface 1*.
8, 9	an RNA detection policy configured to monitor hosts and flow data on the 10.4.0.0/16 network; the policy was applied to a detection engine that used an interface that was migrated to a zone named *interface 3*. Note that this detection policy did not include networks or ports to exclude.
10	a VLAN-filtered intrusion policy targeting VLAN 1 and named *Example Applied VLAN Filtered Policy*; the policy was applied to a detection engine that used an interface that was migrated to a zone named *interface 3*.
11	an unfiltered intrusion policy named *Example Applied Unfiltered Policy;* the policy was applied to a detection engine that used an interface that was migrated to a zone named *interface 3*.
13, 12	an exclusion in the RNA detection policy monitoring network 10.5.0.0/16 to prevent logging connections for TCP port 80 in the network 10.5.2.0/24.
15, 14	an exclusion in the RNA detection policy monitoring network 10.5.0.0/16 to prevent logging connections in the network 10.5.1.0/24.
17, 16	an RNA detection policy configured to monitor hosts and flow data on the 10.5.0.0/16 network; the policy was applied to a detection engine that used an interface that was migrated to a zone named *interface 2*.
18	an unfiltered intrusion policy named *Example Applied Intrusion Policy*; the policy was applied to a detection engine that used an interface that was migrated to a zone named *interface 2*.

Understanding How Interface Sets Become Security Zones

The Version 4.10.3 concept of interface sets is replaced by the Version 5.2 concept of *security zones*, which are groupings of one or more interfaces that you can use to manage and classify traffic flow in various policies and configurations. The interfaces in a single zone may span multiple devices; you can also configure multiple zones on a single device. Using zones allows you to divide the network into segments where you can apply various policies. You must assign at least one interface to a security zone to match traffic against that security zone, and each interface can belong to only one zone. Note that the sensor migration script automatically assigns migrated passive interfaces (but not inline or inline with failopen interfaces) to security zones. See Completing Your Version 5.2 Deployment, page 4-33.

Tip In Version 5.2, an *inline set* refers to one or more pairs of inline interfaces that you group to streamline the applying of various networking settings. Inline sets are unrelated to security zones; not all the ingress interfaces in an inline set must belong to the same zone.

In addition to using security zones to group interfaces, you can use zones in various places in the system's web interface, including access control policies, network discovery rules, and event searches. For example, you could write an access control rule that applies only to a specific source or destination zone, or restrict network discovery to traffic to or from a specific zone.

For each active Version 4.10.3 detection engine in the package you are importing, the configuration import script prompts you to create a security zone on the Defense Center; see Creating Security Zones Based on Interface Sets, page 4-13. Each zone is meant to contain the interfaces in the Version 4.10.3 interface sets monitored by each detection engine.

Note Although the configuration import script can create security zones, if you want to match traffic against those zones you must **manually** assign the interfaces on migrated Version 5.2 devices to those zones **after** you add your migrated Version 5.2 devices to the Defense Center. Note that the sensor migration script automatically assigns passive (but not inline or inline with failopen) interfaces to zones. For more information, see Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33.

When the import script runs, it uses the zones you create to configure rules within the new access control policy and the migrated network discovery rules.

For example, consider a 3D Sensor:

- with an IPS detection engine named `IPS_DE`
- monitoring a inline interface set named `inline_interfaces`
- using an unfiltered intrusion policy named `no_exploits`

If you accept the defaults, the import script:

- creates a Version 5.2 security zone named `inline_interfaces` where you should assign the interfaces that were in the Version 4.10.3 `inline_interfaces` set, and
- creates an access control rule that uses the `no_exploits` intrusion policy to inspect traffic flowing over interfaces in the `inline_interfaces` zone

Tip When configuring a migrated device's interfaces and inline sets, you are **not** required to assign all the interfaces in an inline set to zones created by the import script, although you may want to for the initial configuration and policy apply steps. Zones are meant to group multiple interfaces for security purposes; in practice you might, for example, group all ingress interfaces in the same zone regardless of their inline set. For more information on how interfaces, inline sets, and zones interact in Version 5.2, see the *Version 5.2 Sourcefire 3D System User Guide*.

Understanding How RNA and RUA Settings Are Migrated

In Version 4.10.3, the most critical piece of your RNA deployment is the RNA detection policy. When applied to RNA detection engines on managed 3D Sensors with RNA, the detection policy controls how RNA events and flow data are collected:

- General settings govern policy-specific data collection preferences.
- A list of networks that you specify tells the system which traffic to monitor and log; you can also specify networks that you are monitoring with NetFlow-enabled devices.
- You can specify a list of ports (for specific IP addresses) that you want to exclude from monitoring and logging.

Also in Version 4.10.3, you could collect user activity using 3D Sensors with RUA by creating an RUA detection engine and assigning it to monitor traffic flowing through a specific interface set.

Various settings in the Version 4.10.3 system policy and system settings govern RNA data storage, impact flag correlation, operating system and service identity conflicts, RUA protocol monitoring, NetFlow settings, and so on.

With very few exceptions, Version 5.2 can monitor and log traffic identically to Version 4.10.3, and also adds some capabilities. However, the way you configure discovery (RNA), user awareness (RUA), and connection logging (flow data logging) is now different, and some settings have moved:

- RNA detection policies have been replaced by a single network discovery policy, which you apply to all devices managed by a Defense Center. Using discovery rules, the network discovery policy specifies which security zones, networks, and ports your devices monitor to generate host, application and user data. The network discovery policy includes NetFlow configurations.
- Because you no longer need to configure common settings across multiple detection policies, settings that were in the Version 4.10.3 system policy are now in the network discovery policy.
- You now configure user detection by 3D Sensors wholly within the network discovery policy; any traffic that you can inspect for host data you can inspect for user data. You no longer configure RUA detection engines or restrict detection protocols in the system settings.
- Connection logging (with the exception of NetFlow logging) has moved to the access control policy, where you configure it on a per-access control rule basis. For more information, see Migrating RNA Settings into Rules and Logging Preferences, page 5-7.

Where possible, the configuration import script gracefully migrates your Version 4.10.3 settings to their Version 5.2 counterparts. Your Version 4.10.3 Networks to Monitor settings in your applied RNA detection policies become discovery rules, your old system policy settings are preserved in the network discovery policy, and so on.

Note that in most cases, you will only have one applied detection policy per Defense Center. If you have two applied detection policies, their rules represent a merged version of the networks to monitor, as long as there are no detection engine conflicts in your Version 4.10.3 configurations; see Assigning One Detection Engine of Each Type to Interface Sets, page 4-10. Similarly, if you have existing discovery rules in your Version 5.2 network discovery policy, the migration merges them with the rules it creates.

Note Only user activity detection by 3D Sensors is migrated. User Agent settings and associated LDAP authorization objects are **not** migrated; you must recreate those configurations after the migration.

For more information on how RNA and RUA configurations are migrated, see:

- Understanding How The Migration Creates Discovery Rules, page 5-14
- Migrating Other RNA and RUA Settings, page 5-16

Understanding How The Migration Creates Discovery Rules

The migration process converts the Version 4.10.3 Networks to Monitor and Ports to Exclude settings in your applied RNA detection policies into Version 5.2 discovery rules in the single network discovery policy:

- Each **network** you monitor or exclude creates **one** discovery rule that monitors that network.

  These rules can then be converted to **multiple** discovery rules, depending on your **port exclusions**. The number of rules and the networks monitored by each of the rules depends on the *intersection* of your port-excluded hosts with the networks you were monitoring in Version 4.10.3.

- Each **NetFlow network** you monitor or exclude creates **one** discovery rule that monitors that network.

Discovery rules govern whether and how the system collects information on your network's hosts including the operating systems, active applications, and user activity on those hosts.

Note Version 5.2 discovery rules do **not** govern connection logging for your network traffic; that capability has moved to access control. For more information, see Migrating RNA Settings into Rules and Logging Preferences, page 5-7.

Each discovery rule is also restricted by security zone, which ensures that the system uses the rule to examine only the traffic flowing through certain interfaces. (A zone is a collection of interfaces.)

The following table explains how specific discovery rule settings depend on your Version 4.10.3 configurations. All other settings in the created discovery rules use Version 5.2 defaults. Remember that these settings apply to monitoring **only** and not logging.

Table 5-6 RNA Settings Migrated to Discovery Rules

Version 4.10.3 Policy Configuration	Version 5.2 Discovery Rule Setting	Details
IP Address and **Netmask** in the Networks to Monitor section	**Networks** (Network tab)	Depending on how your Version 4.10.3 networks to monitor intersected with your port exclusions, each discovery rule created by the migration monitors **all or part** of a single network to monitor in Version 5.2.
settings in the Ports to Exclude section, including **Port(s)** and **Protocol**	**Selected Destination Ports** or **Selected Source Ports** (Port Exclusions tab)	Discovery rules created by the migration exclude source or destination ports from monitoring for the rule's specified network depending on your settings in the Version 4.10.3 RNA detection policy.
Exclude data collection option for a network	an **Action** of **Exclude**	If you excluded a network (including a NetFlow network) from monitoring in Version 4.10.3, that network is also excluded in Version 5.2 using a discovery rule with an **Action** of **Exclude**.
Host Data Only or **Host and Flow Data** collection option for a network	an **Action** of **Discover**	If you monitored a network for host data in Version 4.10.3, that network is also monitored in Version 5.2 using a discovery rule with an **Action** of **Discover**. This also applies to NetFlow networks to monitor. This new rule enables both **Hosts** and **Applications** discovery on those networks, to help you build the network map. It also enables **Users** discovery when, in Version 4.10.3, you used an RUA detection engine to monitor the traffic now represented by the discovery rule's security zone restrictions.

Table 5-6 RNA Settings Migrated to Discovery Rules (continued)

Version 4.10.3 Policy Configuration	Version 5.2 Discovery Rule Setting	Details
the **Generate Hosts from NetFlow Data** and **Generate Services from NetFlow Data** general settings	an **Action** of **Log NetFlow Connections** if both these options are disabled	If you had these settings disabled in Version 4.10.3, when the migration creates discovery rules based on your NetFlow networks to monitor, an **Action** of **Log NetFlow Connections** ensures that NetFlow-discovered hosts and applications are **not** added to the network map, but NetFlow connections are still logged.
Reporting Detection Engine for each network to monitor	**Zones** (Zones tab)	Restricting discovery by zone preserves the Version 4.10.3 setting where each network was monitored by a specific RNA detection engine, which would monitor the traffic flowing through a specified interface set. For more information, see Understanding How Interface Sets Become Security Zones, page 5-12. **Note** Subnet detection is **not** supported in Version 5.2 because of the deprecation of detection engines and the new way that you create discovery rules.

Migrating Other RNA and RUA Settings

Various settings in the Version 4.10.3 system policy and system settings govern RNA data storage, impact flag correlation, operating system and service identity conflicts, RUA protocol monitoring, NetFlow settings, and so on.

Migrating NetFlow Settings

The migration transfers the NetFlow-enabled devices you added using the Version 4.10.3 system settings to the Version 5.2 network discovery policy; you configure them on the Advanced tab. Your NetFlow monitoring and flow collection settings are also preserved in discovery rules as described in Understanding How The Migration Creates Discovery Rules, page 5-14. Note that you do **not** need a license for NetFlow data collection in Version 5.2.

Migrating General RNA Detection Policy Settings

The table below summarizes how the migration translates Version 4.10.3 RNA detection policy settings into Version 5.2 settings, most of which are in the network discovery policy. When you run the configuration import script, it overwrites your existing Version 5.2 settings with those in the import package.

Table 5-7 Migrated RNA Detection Policy Settings

Version 4.10.3 Setting	Version 5.2 Setting
Update Interval Capture Banners	You now configure these settings as General Settings on the network discovery policy's Advanced tab. If you import configurations from more than one RNA detection policy, whether in one or different packages: • the new **Update Interval** is the lowest imported value • if any of the Version 4.10.3 policies had **Capture Banners** enabled, it is enabled in Version 5.2
Client Application Detection	Application detection is now configured per discovery rule and cannot be disabled. You can, however, prevent NetFlow-detected applications from being added to the network map by logging connections only.

Table 5-7 Migrated RNA Detection Policy Settings (continued)

Version 4.10.3 Setting	Version 5.2 Setting
Generate Hosts from NetFlow Data Generate Services from NetFlow Data	If you had these settings disabled in Version 4.10.3, when the migration creates discovery rules based on your NetFlow networks to monitor, an **Action** of **Log NetFlow Connections** ensures that NetFlow-discovered hosts and applications are **not** added to the network map, but NetFlow connections are still logged.
Capture HTTP URLs Flow Data Mode Combine Flows for Out-Of-Network Responders	These settings are all logging-related (now handled by access control) and are **not** migrated to the network discovery policy: • In Version 5.2, the **Capture HTTP URLs** setting becomes the **Maximum URL characters to store in connection events** setting, which you configure per access control policy and is enabled by default at 1024 characters. • The other two Version 4.10.3 settings are always enabled in Version 5.2 and therefore you cannot configure them on the web interface. For more information, see Migrating RNA Settings into Rules and Logging Preferences, page 5-7.

Migrating RNA- and RUA-Related System Policy Settings

The table below summarizes how the migration translates Version 4.10.3 system policy configurations into Version 5.2 network discovery policy settings:

- The system policy's RNA Settings migrate to settings on the network discovery policy's Advanced tab.
- The system policy's RUA Settings migrate to settings on the network discovery policy's Users tab.

When you run the configuration import script, it overwrites your current Version 5.2 existing settings with those in the import package.

Table 5-8 System Policy Settings Migrated to Network Discovery Policy Settings

Version 4.10.3 System Policy Setting	Version 5.2 Discovery Policy Setting
RNA Data Storage Settings	Network Discovery Data Storage
RNA Event Logging and Host Input Event Logging	Event Logging Settings
Vulnerabilities to use for Impact Assessment	Vulnerabilities to use for Impact Assessment
Identity Conflict Settings	Identity Conflict Settings
Operating System and Service Identity Sources	OS and Server Identity Sources
RUA Detection Settings	Protocol Detection

Note that the RNA data storage settings that combine flows and drop duplicate events are **not** migrated to the network discovery policy. Not only are these connection logging-related settings (now handled by access control), but in Version 5.2 these settings are always enabled and therefore you cannot configure them on the web interface.

In general, these settings and the way you configure them have not changed from version to version, although much of the discovery-related terminology has changed; see New and Changed Terminology, page 1-2.

Understanding Migrated Intrusion and Audit Events

Optionally, you can migrate legacy intrusion and audit events to your Version 5.2 Defense Center. Field names between the two versions correspond, but keep in mind the following points:

- Information in the intrusion event **Detection Engine** field is migrated to the Version 5.2 **Device** field.
- Any fields added to event tables since Version 4.10.3 are blank in imported legacy events.

Also keep in mind that the timestamps on legacy events will be "behind" newly generated events on the Version 5.2 Defense Center. Because the database is pruned by event timestamp, your migrated events will be pruned before those events.

Tip If imported intrusion events do not display after you complete the import process, clear your browser cache and try again.

Understanding Migrated Compliance Policies and Rules

In Version 5.2, the Policy & Response *compliance* features are collectively known as *correlation*. You can successfully migrate most compliance policies and rules to Version 5.2 correlation policies and rules. Most traffic profiles also migrate successfully.

Note Compliance white lists are **not** migrated.

Version 4.10.3 configurations migrate regardless of whether they are activated; activated configurations in Version 4.10.3 are automatically activated in Version 5.2 by the migration process.

So that your Version 5.2 correlation configuration can behave equivalently to your Version 4.10.3 deployment, the migration must update configurations that use detection engine constraints. A Version 4.10.3 compliance rule based on an intrusion or flow event that uses a **Detection Engine** constraint becomes a Version 5.2 correlation rule based on an intrusion or connection event that uses a **Security Zone** constraint. Restricting correlation rules by zone preserves the Version 4.10.3 setting where a detection engine monitors the traffic flowing through a specified interface set. For more information, see Understanding How Interface Sets Become Security Zones, page 5-12.

Also note that compliance conditions reflect terminology changes. For example, a Version 4.10.3 compliance condition with a **Service**, **Client Application**, or **Payload** constraint becomes a Version 5.2 condition with an Application Protocol, Client, or Web Application constraint. For more information, see New and Changed Terminology, page 1-2.

The Policy & Responses configurations that you **cannot** migrate are detailed in the following table. Both the configuration export and import scripts warn you that these configurations will not be migrated, and give you a chance to exit the script.

Table 5-9 Unsupported Conditions in Compliance Rules and Traffic Profiles

You cannot migrate a...	Where...	Because...
compliance rule	**an RNA event occurs** using a **Detection Engine** constraint	the migration script cannot create a Version 5.2 discovery-based correlation rule using a **Device** constraint until you add devices to the Defense Center, which you do after you run the import script. You can create these configurations after you complete the migration process.
compliance rule	**an RNA event occurs** or **a flow event occurs** using an **Application Type** or **Payload Type** constraint	in Version 5.2, you cannot trigger correlation rules based on application categories and tags, which are the Version 5.2 analogs for application and payload types.
traffic profile	a host profile qualification using a **Client Application** constraint where you specify one or more **Application Type** (other than **any**)	in Version 5.2, you cannot track connections based on application categories and tags, which are the Version 5.2 analogs for application and payload types.
traffic profile	a host profile qualification using a **Client Application** constraint where you specify an **Application** of **any**	in Version 5.2, you cannot track connection based on a **Client** of any; you must explicitly choose one or more client applications.

Changes to eStreamer Syntax and Data Structures

With each release of the system software, several of the eStreamer data structures change. To determine whether each of the data structures your client currently receives is the current version of that structure, review the tables in the Host Discovery and Connection Data Blocks, Intrusion Event and Metadata Record Types, and Understanding Host Data Structures chapters in the Version 5.2 *Sourcefire 3D System eStreamer Integration Guide*. If it is not, update your client to reflect the current structures.

In addition, you should review the Understanding the eStreamer Application Protocol chapter in detail to understand the new types of information available in Version 5.2 and how to request them.

Note Version 4.10.3 eStreamer settings on your appliances are **not** migrated. After you complete the migration process, you must re-enable the streaming of specific event types to eStreamer clients before you can request data, as well as add the client to the eStreamer server's peers database on the Defense Center. For more information, see the *Version 5.2 Sourcefire 3D System User Guide*.

For a summary of the major changes to eStreamer, see the following sections.

Series 2 Data Structures and Extended Requests

Series 2 data blocks were introduced in Version 5.0 and have a separate numbering system from series 1 data blocks. These blocks contain discovery and connection data and were previously known as RNA data structures.

Use *extended requests* to request information, such as Series 2 data blocks, that is not available from normal requests. Submit extended requests by setting bit 30 in the Event Stream Request message. When this bit is set, eStreamer responds with a list of available services. The client returns a Streaming Request message that indicates the service it wants to use, with a request list of event types and versions available from that service.

The eStreamer server sends messages in a bundle format when the client submits an extended request. The client responds with a NULL message to acknowledge receipt of an entire bundle. The client should not acknowledge receipt of individual messages in a bundle.

Alternate Ports

You can now configure eStreamer to use a port other than the primary management port.

IPv6 and Geolocation

Numerous data blocks now include source and destination countries for use with the geolocation feature. Also, all IP address fields now support both IPv4 and IPv6 addresses.