Firewall rules creation process

**Preliminary:** only Cisco interfaces that have both name and IP address defined, are valid for rule-base conversion process –

*interface GigabitEthernet0/0.556*

*vlan 556*

***nameif 0556\_CNN\_DMZ\_NET\_ThinktelSIPMPLS***

*security-level 50*

***ip address 206.80.252.190 255.255.255.252***

Otherwise, commands that reference invalid interface are not converted and the user is alerted.

1. **Rules created from inbound access-group commands**

The tool loops over all valid ***access-group*** commands and per each command creates a sub-policy (inline-layer) using an interface name referenced in the command.

Only inbound (“in”) commands are processed – outbound (“out”) commands are skipped and the user is alerted.

If the interface referenced in the access-group command is management-only interface (“management-only”) and a ***hostname*** command exists, a first rule called “Automatic rule for management-only interface” is created –

*source: any*

*destination: hostname-command-value*

*destination-negated: true*

*service: any*

*action: drop*

Then, using the access-group command’s name as a reference, it locates all relevant access-list commands and adds them to the sub-policy.

If there is no cleanup access-list command, an automatic cleanup rule is created and added at the end.

1. **Rules created from interface commands**

The tool loops over all valid ***interface*** commands and per each command that has no valid inbound access-group defined and its security-level is above 0, it creates a sub-policy (inline-layer) using an interface name referenced in the command.

Then, per each interface above, it loops again over all other valid interface commands and creates a rule for an interface with lower security-level –

*source: any*

*destination: interface-name*

*service: any*

*action: accept*

Finally, an automatic cleanup rule is created and added at the end.

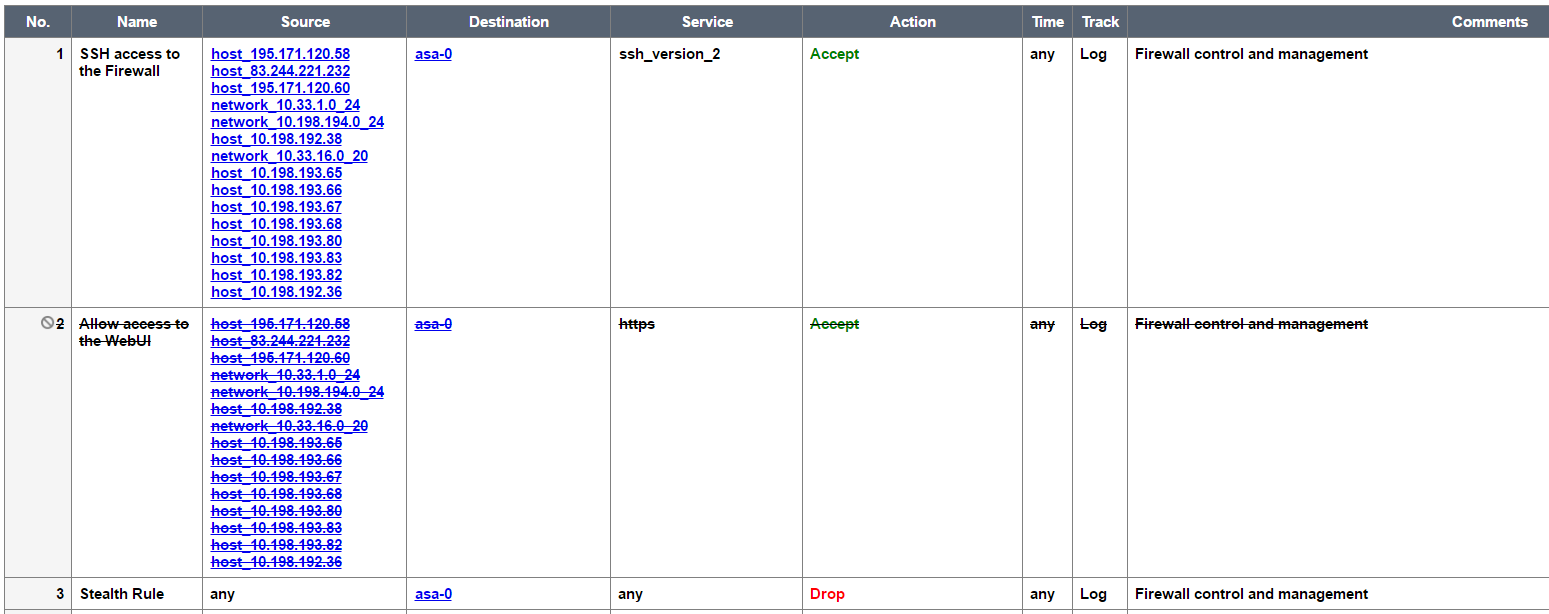
Interfaces defined as management-only, are skipped in this process.

1. **Global rules created from outbound access-group commands**

All global ACLs are added at the end of each sub-policy, just before the cleanup rule.

1. **Rules created due to Cisco SSH OS commands for firewall control and management**

These rules will be the top rules in the policy –



1. **General notes**

* Rules that stand for interface marked as “shutdown” are created as disabled.
* Services referenced in ACL are added as a flat (service groups are flattened) services list to the firewall rule.