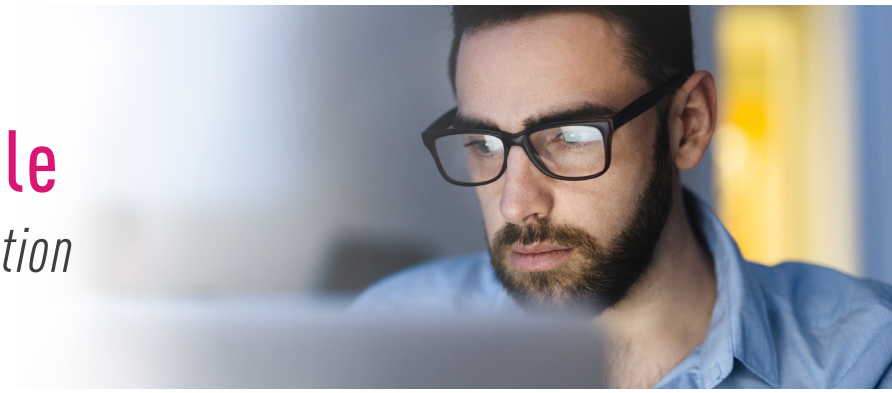
Check Point + Ansible

Accelerate Cyber Threat Prevention



Challenge

For a long time now, many security veterans have been urging organizations of all sizes to implement security processes earlier in the software development lifecycle (SDLC) to improve the effectiveness of both application and operational security. The move to DevSecOps presents a unique opportunity to finally make security 'shift left' of the SDLC process chain, because with this methodology, improvement of all types is continuous. There is no 'end' of development to tack security onto, so the only way it is going to effectively be implemented into the flow is if it is embedded throughout.

How can we integrate IT security teams and the security solutions they use in a fast-paced environment?

Solution

Integrating through application programming interfaces (APIs) in Check Point, the Red Hat® Ansible® Automation Platform provides a framework for codifying processes into an automated workflow, freeing SOC and IT security teams to concentrate on more critical tasks.

KEY PRODUCT BENEFITS

- **Reduce Incident Analysis Time:** Automated tools can collect data about security threats from multiple sources without human assistance, reducing overall investigation analysis time.
- **Automate Incident Response:** Seamlessly trigger mitigation policies on Next-Gen Threat Prevention firewalls
- **Automate Routine Tasks:** Reduce the time it takes to maintain large, distributed security deployments.
- **Improve Speed and Agility:** Rapidly provision both physical and virtualized next-generation firewalls.
- **Configure with Confidence:** Apply the security you need in a simple, consistent, manner.

Including Security in the CI/CD Pipeline

The Check Point Ansible network modules fit tightly into the DevOps lifecycle Continuous Integration/Continuous Deployment pipeline. Gone are the days of hand-typing commands into security devices one by one. Manage your security infrastructure using Ansible and Check Point modules throughout the entire production life cycle:

- Configuration automation
- Test driven deployment
- Continuous compliance

Ansible's simple automation framework means that previously isolated security operators can finally speak the same language of automation as the rest of the IT organization. Check Point Next Generation Firewalls can now be included in an organization's overall automation strategy for a holistic approach to application workload management.

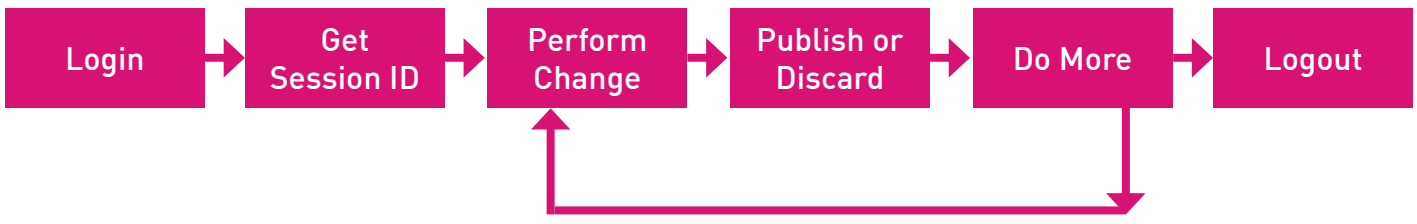
Automate Securely

With Ansible Tower credentials for machines and cloud systems are stored securely in a powerful role-based access control engine that allows you to easily set policies on who can run what automation in what environments, ensuring that only the proper people have the ability to access machines and apply configuration.

Check Point Security Management also allows multiple administrators to work simultaneously with no conflicts. To avoid configuration conflicts, all work is done in sessions where objects are locked when modified. Other administrators working in SmartConsole will see that the object is locked and will not be able to change it until the session locking the object is published or discarded. This client-server design enables opening multiple sessions in parallel allowing concurrent access. If there is an accidental disconnection, then no work is lost.

Check Point Security Management also enables delegation through permission profiles and unified policy layers that provide the ability to separate the policy into independent segments, which can be independently managed and automated.

The operational flow is exactly the same for the API as it is for SmartConsole, i.e. Login > Get Session > Do changes > Publish > Logout. More information on how to use HTTP-based RESTful API calls is available in the Security Management API online reference guide. These APIs are the basis for new Check Point Ansible Collections that are available for Ansible.



Trust, Yet Verify Compliance

Once you've defined your security configuration, you need to be able to verify it and verify it on a consistent basis. Ansible's idempotent nature means you can repeatedly apply the same configuration, and it will only make the necessary changes to put the system back into compliance. By investigating these runs, you can easily see where changes are needed.

Summary

Not only must you be able to define what it means for your systems to be secure, you need to be able to simply apply that security, and constantly monitor your systems to ensure they remain compliant with that security. Moving to using automation as part of your IT practices is a necessary first step for security. The proper automation tooling allows you to apply the security you need in a simple, consistent, manner, allowing you to concentrate on other things.

Use Cases

Driving automated threat prevention and security policy orchestration is key to protecting your organization from the expanding threat landscape. Other use cases include automating security maintenance of both physical and virtualized next-generation firewalls.

Security Automation with Check Point and Ansible

With Ansible you can automate and integrate Check Point and other security solutions to accelerate the investigation and response to threats across the enterprise in a coordinated, unified way using a curated collection of modules, roles and playbooks.

Triage of Suspicious Activities

Collect logs across Check Point Next Generation Firewalls and other security systems programmatically, enabling on-demand enrichment of triage activities performed through security information and event management systems (SIEMs).

```
---
- name: Send Check Point logs to SIEM syslog
  hosts: check_point_host
  collection:
   - check_point.mgmt
  vars:
   syslog_server: mysiem.example.com
    checkpoint_server_name: "gw-1g3f5"
    firewall_provider: checkpoint
  tasks:
    - include_role
        name: ansible_security.log_manager
        tasks_from: forward_logs_to_syslog
```

Threat Hunting

Automatically tune the level of logging, create new intrusion detection system (IDS) rules and new firewall policies facilitating the detection of more threats in less time.

```
---
- hosts: check_point_host
  connection: httpapi
  collection:
    - check_point.mgmt
  tasks:
  - name: Add threat rule in IDS
    cp_mgmt_threat_rule:
      install_on: myngfw
      layer: Network
      name: "ids-rule"
      position: top
      protected_scope: All_Internet
      state: present
      auto_publish_session: true
```

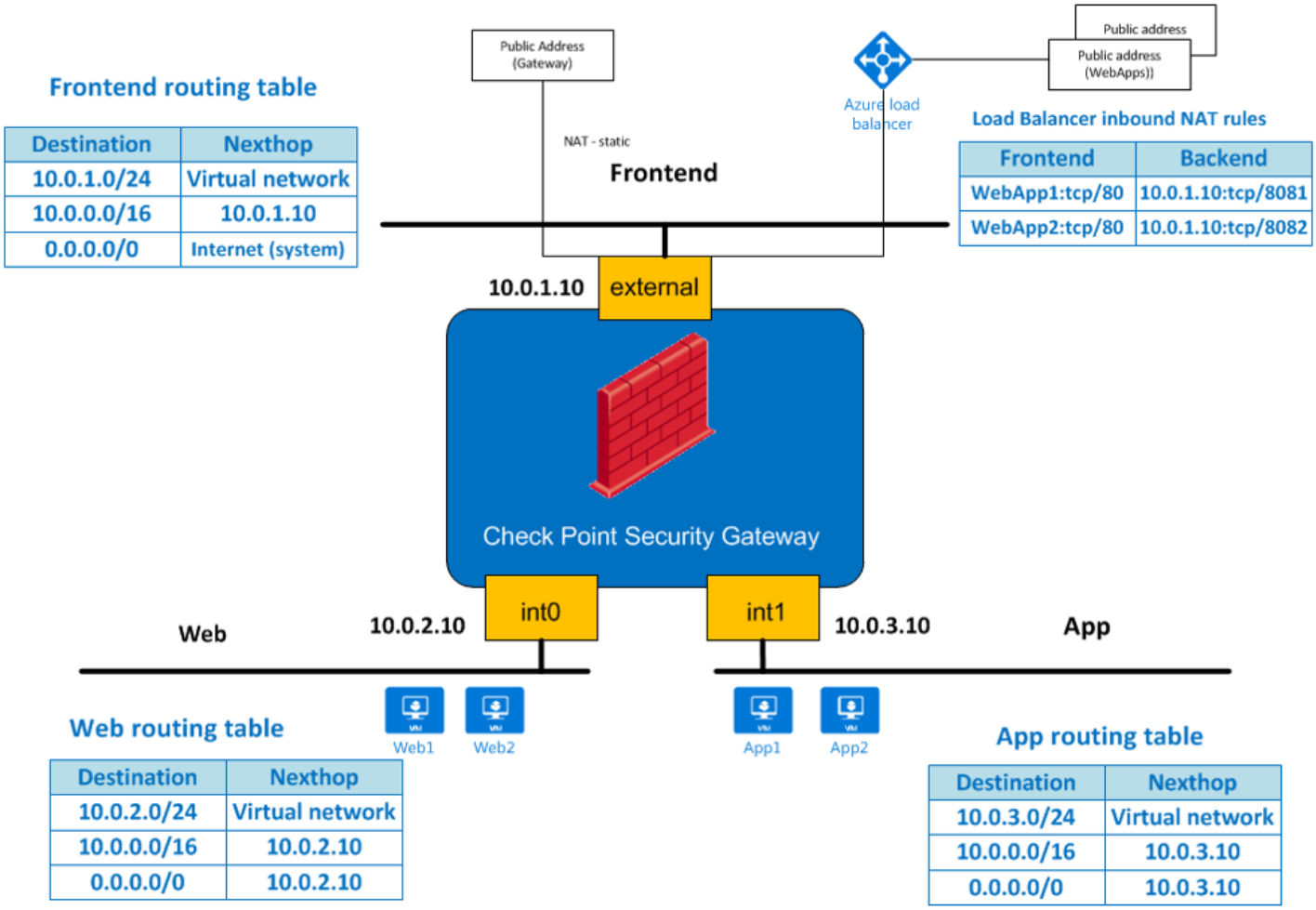
Incident Response

Remediate faster automating actions like blacklisting attacking IP addresses or domains, whitelisting non-threatening traffic, or isolating suspicious workloads for further investigation.

```
---
- name: Blacklist attacker
  hosts: check_point_host
  collection:
    - check_point.mgmt
  vars:
    source_ip: 11.22.33.44
    destination_ip: 192.168.23.44
  tasks:
    - name: Create blacklist entry
      cp_mgmt_access_rule:
        auto_install_policy: yes
        auto_publish_session: yes
        layer: Network
        position: top
        name: "blacklist_policy"
        source: "asa-{{ source_ip }}"
        destination: "asa-{{ destination_ip }}"
        action: drop
```

Cloud Provisioning

From traditional bare metal through to serverless or function-as-a-service, automating the provisioning of any infrastructure is the first step in automating the operational life cycle of your applications. Ansible can provision the latest cloud platforms, virtualized hosts and hypervisors, network devices and bare-metal servers. Provisioning cloud instances is a perfect Check Point and Ansible use case. When needed, create a Virtual Private Cloud (VPC), install a web server and configure a Check Point security gateway policy in one playbook.



Configuration Management

Ansible is the simplest solution for configuration management available. It's designed to be minimal in nature, consistent, secure and highly reliable, with an extremely low learning curve for administrators, developers and IT managers. Ansible configurations are simple data descriptions of your infrastructure - ensuring everyone on your team will be able to understand the meaning of each configuration task.

With the Check Point and Ansible solution admins can automate the process of installing software updates using Ansible and the Check Point Security Management APIs.

```
---
hosts: check_point_host
connection: httpapi
collection:
    - check_point.mgmt
tasks:
  - name: show available HFs
    cp_mgmt_show_software_packages_per_targets:
    register: install_response

  - name: Verify Jumbo HF
    cp_mgmt_verify_software_package:
      name : "Check_Point_R80_20_JUMBO_HF_MAIN_Bundle_T8_FULL.tgz"
      targets :
        - "R80_20_DemoGW"
    when: install_response.failed == false
    register: verify_response

  - name: Install Jumbo HF
    cp_mgmt_install_software_package:
      name : "Check_Point_R80_20_JUMBO_HF_MAIN_Bundle_T8_FULL.tgz"
      targets :
        - "R80_20_DemoGW"
    register: verify_response
```

Check Point Ansible Gaia Collection

The GAiA Ansible collection provides control over Check Point firewalls using the Check Point GAiA API. One use case is automating the configuration of the first time configuration which is run when deploying a new Check Point device in the network.

```
---
- name: Run First Time Wizard configuration.
  hosts: check_point_host
  connection: httpapi
  collections:
    - check_point.gaia
  tasks:
    - name: Run First time Wizard (Initial Setup)
      cp_gaia_initial_setup:
        wait_for_task: True
        security_management: {
            multi_domain: False,
            # Type choices: 'primary', 'secondary', 'log-server', default='primary'
            type: primary,
            activation_key: vpn123,
            leading_interface: "eth0",
            gui_clients:
              {
                range:
                  {
                    "first_IPv4_range": "10.0.1.0",
                    "last_IPv4_range": "10.0.1.200",
                  },
              },
          }
        # Possible Gui Clients options:
        # network: { "address": "10.0.0.0", "mask_length": "8" },
        # single_ip: "10.0.1.131",
        security_gateway:
          {
            cluster_member: False,
            activation_key: vpn123,
            dynamically_assigned_ip: False,
          }
      register: FTW_results
    - name: print FTW response
      debug:
        msg: "{{ FTW_results }}"
```

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 www.checkpoint.com