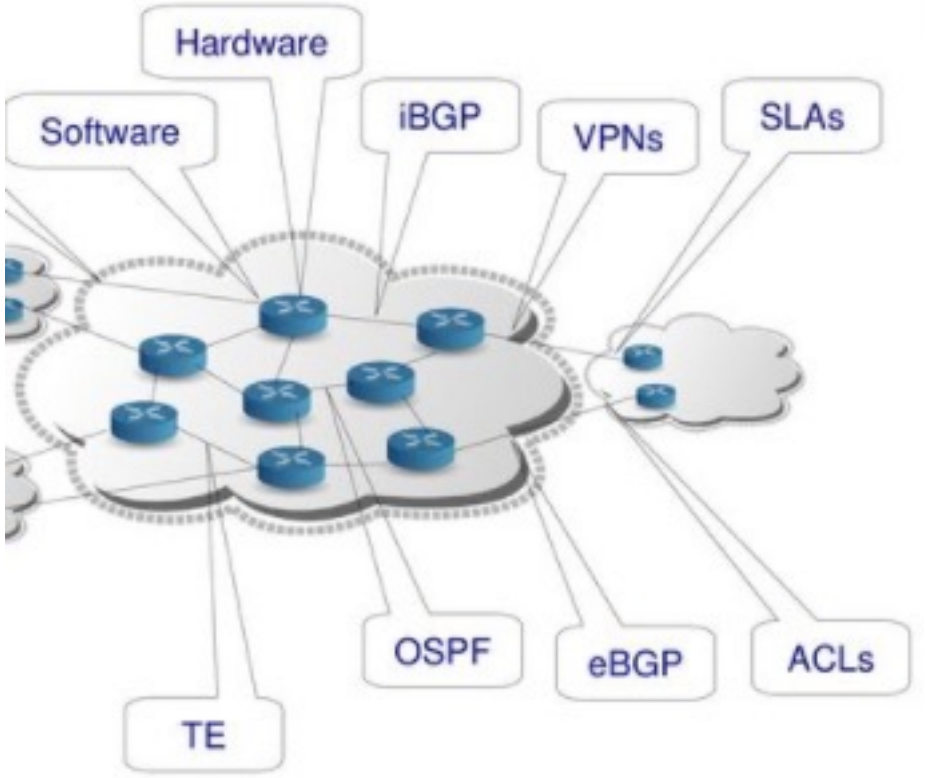
Gerência de configuração (CM)

Backups de configurações de rede, automação da rede, controle de alterações de configuração, recuperação de falhas e auditoria.

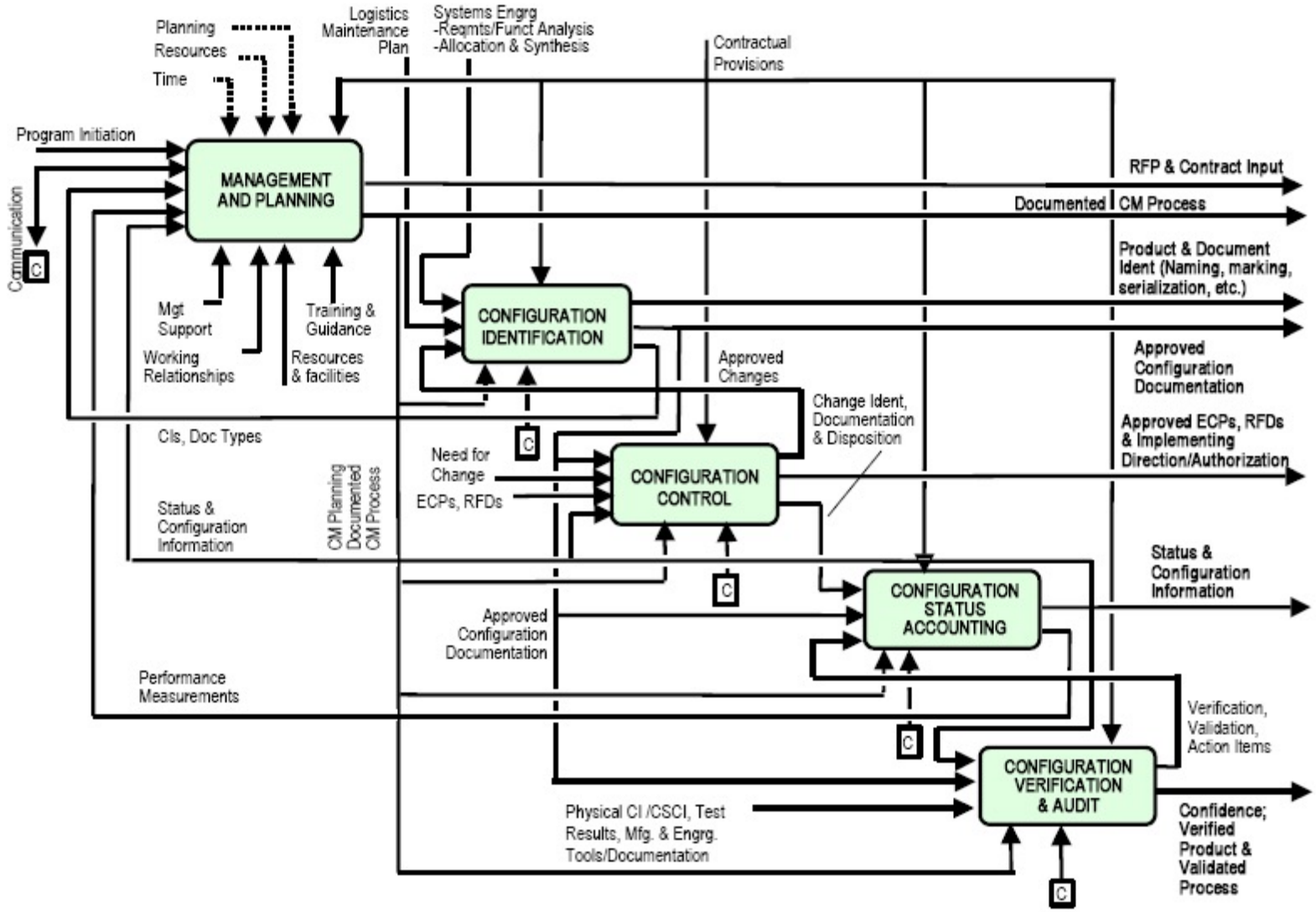
Porque gerenciar configurações

- Automação de processos
- Padronização de configurações
- Gerencia de mudanças
- Facilidade de rollback
- Reduz riscos de segurança
- Auditoria de configurações



- DevOps estão se tornando responsáveis por essa área!

O mundo ideal da gerência de configurações



Cuidado!

Gerência de configuração normalmente significa

“Ferramenta de acesso remoto com poder de administrador”

Gerência de configuração: O básico para qualquer ASN

- Controle de acesso aos equipamentos de rede
  - **Autenticação centralizada** LDAP, radius
  - Restrição de acesso a rede out-of-band (OOB)
- Controle de alterações de configuração
  - restrições de usuários e atividades
  - **Templates de usuários** – operador, admin, devops
  - Facilidades para permitir / retirar acesso a equipamentos
- Suporte a **Commit / Rollback** de configurações em equipamentos
  - Controle de versão de software
  - Controle de versão de configurações (roteadores, switches, DNS, etc.)
- **Logs** de configs para a auditoria

Gerência de usuários dos eqtos de rede (controle de admissão)

- Mobilidade considerável na área de TI
- Não esqueça de gerenciar quem tem acesso a seus equipamentos
  - Radius / LDAP é necessário
  - Controle central de usuários
- **Senhas 'padrão' não são aceitáveis**

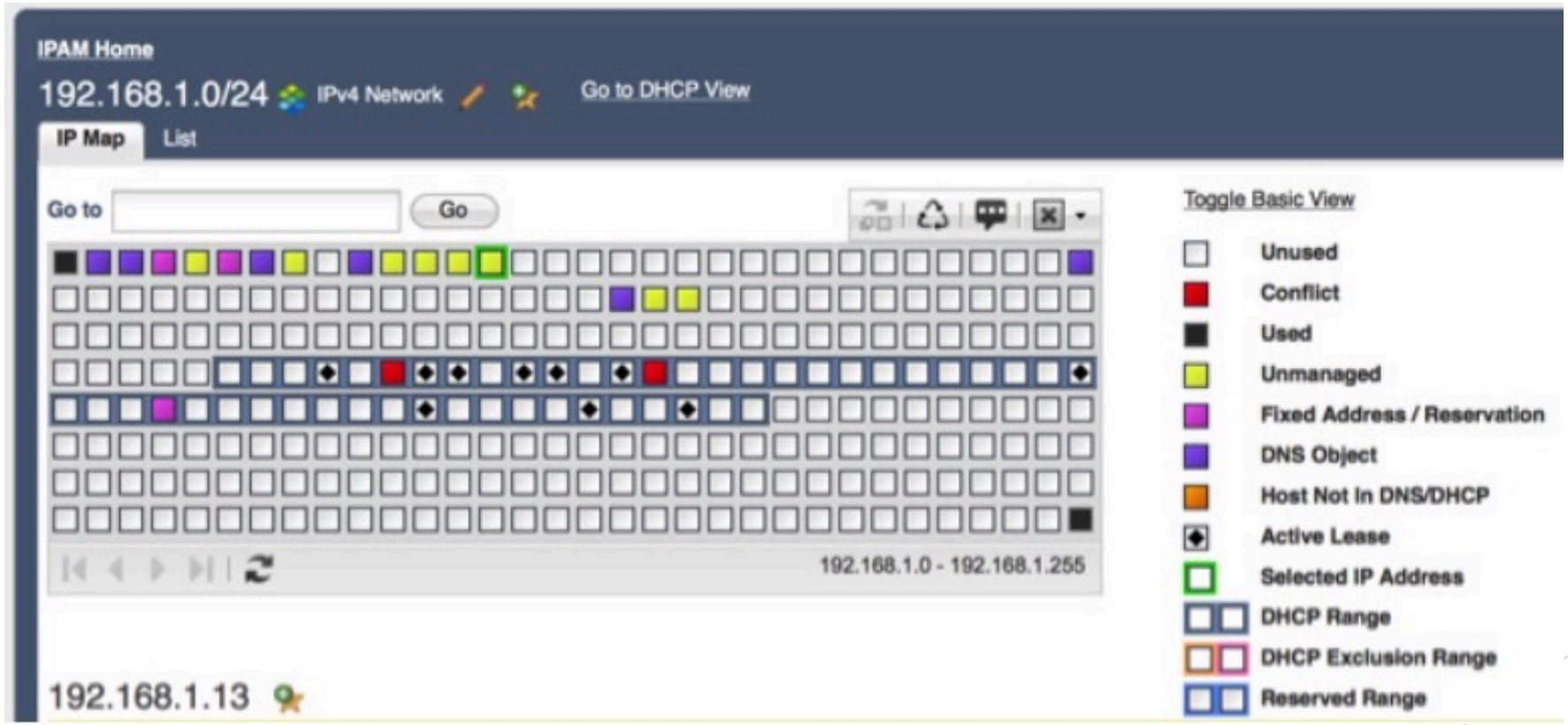
Table 4. System actions performed by attackers.

	message	count
1	new script scheduled by admin	154
2	PPTP server settings changed by admin	63
3	L2TP server settings changed by admin	50
4	SSTP server settings changed by admin	38
5	DNS changed by admin	25
6	DHCP client changed	21
7	PPTP server settings changed	19
8	SSTP server settings changed	19
9	L2TP server settings changed	19
10	PPP profile <default-encryption>changed by admin	19

Leitura: Characterising attacks targeting low-cost routers: a MikroTik case study

Gerência de endereçamento IP

https://phpipam.net/



Interfaces para gerência de configuração

- O mais comum em softwares para gerência de configuração (CM)
  - Acesso SSH para equipamentos
  - Opte por usar chaves publicas/privadas para autenticação
- Agentes próprios da aplicação CM
  - Necessário instalar em servidores
  - Lembre-se de restringir portas de acesso

Ferramentas usadas para gerência de configuração (Orquestração)

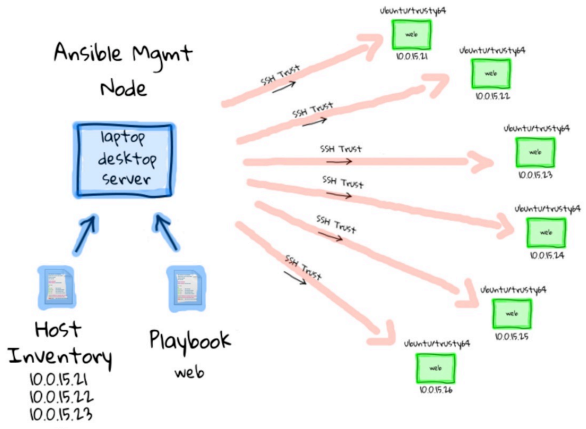
- Ansible (https://ansible.com/community)
- Puppet (https://puppet.com/community/)
- Hashcorp Terraform (https://terraform.io)
- Saltstack (https://saltproject.io/)
- Rconfig (https://www.rconfig.com/)
- CFEngine
- Microsoft System Center Configuration Manager

- Ou você mesmo pode programar
  - Python – paramiko library
  - Exemplo: https://github.com/LMBertholdo/TANGLED-cli

ansible

https://github.com/ansible/ansible

- **Utiliza “playbooks”**
- **Um playbook contém várias tarefas**
- **Sintaxe em YAML**



YAML playbook

```yaml
---
- name: "Create directory structure"
  hosts: localhost
  tasks:
  - name: "Instantiate"
    file:
      path: "{{ item }}"
      recurse: true
      mode: "u=rwx,g=rwx,o=r"
      state: directory
    with_items:
      - "foo/src"
      - "foo/dist"
      - "foo/doc"
```

```yaml
- name: configure top level configuration
  cisco.ios.ios_config:
    lines: hostname {{ inventory_hostname }}

- name: configure interface settings
  cisco.ios.ios_config:
    lines:
    - description test interface
    - ip address 172.31.1.1 255.255.255.0
    parents: interface Ethernet1
```

```yaml
- name: load new acl into device
  cisco.ios.ios_config:
    lines:
    - 10 permit ip host 192.0.2.1 any log
    - 20 permit ip host 192.0.2.2 any log
    - 30 permit ip host 192.0.2.3 any log
    - 40 permit ip host 192.0.2.4 any log
    - 50 permit ip host 192.0.2.5 any log
    parents: ip access-list extended test
```

access-list extended test

```yaml
- name: check the running-config against master config
  cisco.ios.ios_config:
    diff_against: intended
    intended_config: "{{ lookup('file', 'master.cfg') }}

- name: check the startup-config against the running-con
  cisco.ios.ios_config:
    diff_against: startup
    diff_ignore_lines:
    - ntp clock .*

- name: save running to startup when modified
  cisco.ios.ios_config:
```

Gerência de configuração