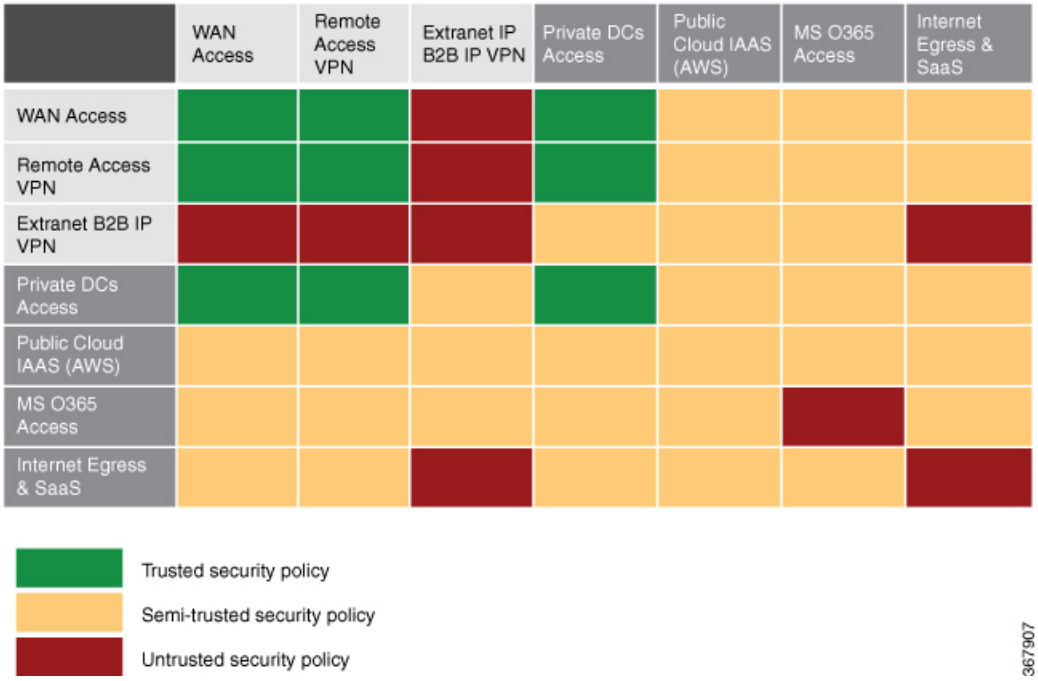
Service Design

An enterprise would typically go through the following stages while designing their service for SAE.

Identify VNFs

The following connection patterns emerge from the analysis of Acme Corp's consumers and providers.



The table above shows which groups cannot interact with each other (red), which groups can interact, but with certain controls (orange), and which groups can interact without additional security services (green).

Partners accessing application through MPLS, WAN, Internet, and employees represent the consumers.

How to Identify VNFs for your Design

The type of VNFs you need depends on your traffic patterns and volume. For example, if you are creating a consumer chain for traffic coming from your employees, you require fewer firewalls as the source of such traffic is considered to be trusted.

SAE supports both–Cisco VNFs and third-party VNFs supported by Cisco. Based on your traffic patterns and volume, select the VNF that suits you best. The following are some possible options.

- Routing: CSR
- Firewall: FTDv, ASAv, Palo Alto Firewall
- Load Balancing: AVI, F5

VNF features and licensing costs are the additional criteria that you must consider while selecting the VNFs for your service chains.

See Cisco CSP 5000 Series Datasheet for a complete list of supported VNFs.

Design Service Chains

Consumers and providers interact with each other through a set of service chains. Service chains are built by connecting VNFs together.

About Service Chains

Service chains are designed to meet the traffic flow discovered in the audit phase. The service design is based on your connection patterns and security policies. Security policies depend on the trust level of the connections. Therefore, the design of your service chains also depends on the following.

- Trust level of your connections
- The security policies you wish to apply to your connections
- The bandwidth associated with your traffic flows

You must consider the following factors while designing your service chains.

- SR-IOV versus DPDK: Your service chain design depends on the VNFs that you have identified and their support in each of these modes.
- High Availability (HA)
- Port channel
- Licensing

Design SAE Site

The number of CSP devices required for your SAE site depends on the following:

- Number of service chains required for your enterprise traffic
- VNFs in each service chain and their bandwidth requirements

- Throughput per service chain
- Cores per site and NIC types

Switching Requirements

- The switches must be in VEPA mode to enable visibility into the traffic.
- Whether the switching fabric is in standalone mode or spine-leaf mode depends on the number of port requirements that your design requires.