Contents

Summary

As communications infrastructures continue to evolve, email has become a critical component to business processes. The level of sophistication of what has come to be known as Spam Mail and Virus/Trojan applications have also evolved. Many companies now regularly report that up to 90% of in-bound email messaging has nothing to do with business. To deal with this issue that impacts not only available bandwidth resources, but also message storage on Servers and SANs, companies both large and small have turned to Email Security and Scanning solutions to minimize the impact of malicious email.

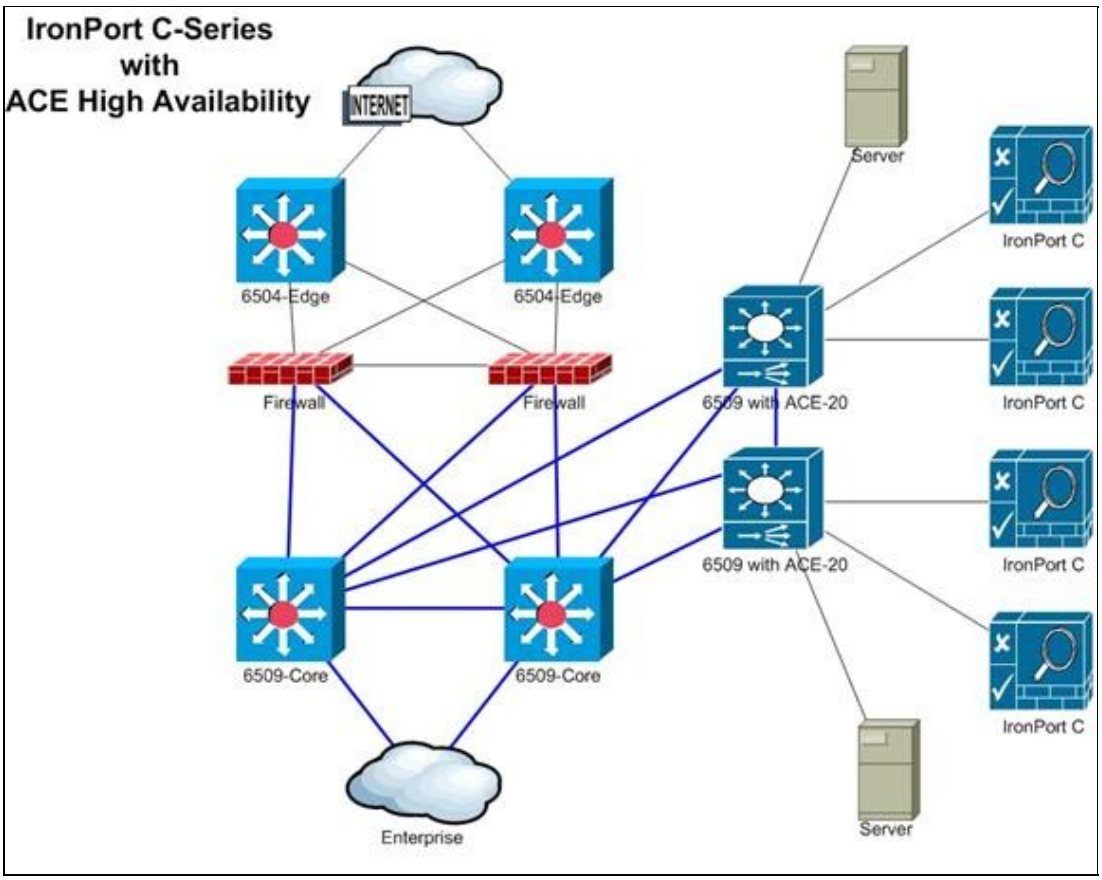
IronPort email security appliances combine market-leading, best-of-breed anti-spam, antivirus, encryption, digital rights management, and archiving technologies. These solutions run on IronPort?s revolutionary MTA platform, providing the highest levels of email protection, with exclusive preventive and reactive technologies, and industry-leading email management tools.

When coupled with the Application Control Engine, the solution now scales to meet virtually any size solution. ACE brings high-availability and additional levels of security to the overall solution. The Cisco ACE, either the module for Catalyst 6500 chassis, or the 4710 Appliance provide industry leading capabilities including virtual execution environments, roles-based administration, and scalability via licenses not forklift hardware changes.

Overview

This document will discuss a particular deployment of IronPort C-Series appliances along with ACE. The ACE provided the High Availability environment for a total deployment of 4 Iron Port appliances. It was also inserted into the data path without impact to the existing infrastructure.

The flexibility for deployment of ACE, coupled with industry leading features has positioned this deployment to be one of over 100 applications to be addressed at this particular customer. The base infrastructure of this installation looks like this:



Of note are the blue links that are 802.1Q trunks allowing the transparent Firewalls to provide L2 access to the Edge Catalyst 6509 switches, thus the ACE VIP is a Public IP address.

Prior to adding ACE into this solution the customer needed a way to effectively provide High Availability for email scanning via the IronPort appliances. ACE effectively provided not only the Virtual IP address, but also enforced additional security features into the solution which were not provided by the Firewalls or existing infrastructure. These additional security features include the ability to enforce TCP/IP Normalizations for

- Bad segment checksum
- Bad TCP header or payload length
- Suspect TCP flags (for example, NULL, SYN/FIN, or FIN/URG)

These are on by default and are handled at the VLAN interface. ACE will always drop this traffic and can be configured for more in-depth protocol enforcement via parameter maps. In addition, ACE also employs ICMP-Guard, SYN-Cookie (Anti-DDoS), IP TTL, and uRPF for securing the overall environment.

ACE utilizes device virtualization by means of contexts, much the same as the Firewall Services Module and ASA products. Each of these contexts provides an independent execution space for packet and flow processing. The Admin context acts much like the Control Plane for the ACE device as it is where other contexts are defined, failover options for High Availability, and devices resources are configured and provided to other virtual contexts. Here is the Admin context configuration for this solution:

```
SF_ACE/Admin# show running-config
  Generating configuration....
```

```
  login timeout 0
  hostname SF_ACE
  boot system image:c6ace-t1k9-mz.A2_1_1.bin(ACE module ver. 2.1)

  resource-class IP-rsc
    limit-resource sticky minimum 5 maximum equal-to-min
```

(required since sticky [session persistence] is required for the solution. The sticky resource does not grow between a min and a max like the other ones. It will allocate the minimum and this is all you get. So make sure you allocate enough sticky resource.)

```
class-map type management match-any remote-access
    2 match protocol ssh any
    3 match protocol snmp any
    4 match protocol https any
    5 match protocol telnet any
    6 match protocol icmp any

  policy-map type management first-match remote-mgmt
    class remote-access
      permit

  interface vlan 207
    description Management Side
    ip address x.x.207.21 255.255.255.0
    peer ip address x.x.207.22 255.255.255.0
    alias address x.x.207.20
    service-policy input remote-mgmt
    no shutdown

  ip route 0.0.0.0 0.0.0.0 x.x.207.1

  context IronPort
    allocate-interface vlan 208
    member IP-rsc
```

(tying resource-class to the context)

```
username admin password 5 (removed)  role Admin
  domain default-domain
  username www password 5 (removed)  role Admin domain default-domain
```

In order to properly segment the traffic from the Admin context (Control Plane) a context called IronPort was created as shown above. Here is the configuration of the IronPort context:

```
SF_ACE/IronPort# show running-config
  Generating configuration....


  access-list ALL line 10 extended permit ip any any


 probe tcp IP-pro
  description IronPort Probe
  port 25
  interval 10
  faildetect 5
  passdetect interval 15
  passdetect count 5
```

```
receive 20
```

(Provides a keepalive probe every 10 seconds and expects a response within 20 seconds. If an IronPort is off-line, it will be put back into service after 75 seconds from initial good contact on port 25)

```
rserver host IP1
  ip address x.x.208.225
  inservice
rserver host IP2
  ip address x.x.208.226
  inservice
rserver host IP3
  ip address x.x.208.230
  inservice

serverfarm host IP_SF
  predictor least-conns
 probe IP-pro
  rserver IP1
    inservice
  rserver IP2
    inservice
  rserver IP3
    inservice

sticky ip-netmask 255.255.255.0 address source STICKY-grp
  timeout 120 (suggested max timeout for IronPort sessions)
  replicate sticky(insures that sessions are sent to the same server)
  serverfarm IP_SF (ties the sticky sessions to the serverfarm)




class-map match-any IPVIP-cls
  2 match virtual-address x.x.208.233 tcp eq smtp (mail traffic only)
class-map type management match-any MGMT-cls
  3 match protocol https any
  4 match protocol icmp any
  5 match protocol snmp any
  6 match protocol ssh any
  7 match protocol telnet any
  8 match protocol http (required for Iron Port updates)

policy-map type management first-match MGMT-pol
  class MGMT-cls
    permit

policy-map type loadbalance first-match IPLB-pol
  class class-default
    sticky-serverfarm STICKY-grp

policy-map multi-match IPVIP-pol
  class IPVIP-cls
    loadbalance vip inservice
    loadbalance policy IPLB-pol
    loadbalance vip icmp-reply active
    nat dynamic 1 vlan 208
```

(SNAT required due to one-armed mode for traffic to return correctly to ACE from Iron Port appliances)

```
service-policy input MGMT-pol
access-group input ALL
```

```
(putting both in the global configs means they apply to all interfaces)

interface vlan 208
  ip address x.x.208.252 255.255.255.0
  peer ip address x.x.208.251 255.255.255.0
  alias address x.x.208.250
  nat-pool 1 x.x.208.253 x.x.208.253 netmask 255.255.255.0 pat
  service-policy input IPVIP-pol
  no shutdown

ip route 0.0.0.0 0.0.0.0 x.x.208.1
```

Of interest to note is the One-Armed configuration of the IronPort context above. This was provided to minimize the impact to the existing environment as the IronPort appliances are accompanied by other devices on that segment. As previously mentioned, SNAT is used to insure that traffic on port 25 destined to the Iron Port appliances is returned to the ACE and not the default gateway which is x.x.208.1. Also note that the base ACE security features are enabled on the VLAN208 interface, Normalizations and ICMP-Guard. These are features not provided by the transparent firewall at the Internet Edge.

Conclusion

The combination of IronPort and ACE products makes for a compelling event for many customers. Iron Port providing, in this case, email security and ACE providing the scalability and high availability with minimal impact to the existing infrastructure. This also positions the customer to grow the applications serviced in a similar mode by ACE with additional features and operations not mentioned here and each in their logical execution space via virtual contexts. All this while scaling from the current 4Gbps throughput license to 16Gbps, 15,000 SSL transactions per second, and up to 250 virtual contexts without upgrading hardware.

Related Information

Technical Support & Documentation - Cisco Systems

ACE: http://www.cisco.com/en/US/products/ps6906/index.html

http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

IronPort: http://www.ironport.com/products/email_security_appliances.html