開
放
的
열린
مفتوح
libre
मुक्त
ಮುಕ್ತ
livre
libero
ముక్త
开放的
açık
open
nyílt
פתוח
オープン
livre
ανοικτό
offen
otevřený
öppen
открытый
வெளிப்படை

open

USE IMPROVE EVANGELIZE

Practical (Open)Solaris Security

Brent Paulson
Solaris Sustaining
Sun Microsystems, Inc.

Source Material for This Presenation Came Largely From:

- http://opensolaris.org/os/community/security/preso/

Primarily the following presentations:

- **Hack-Fu - Deconstructing the Security Capabilities of the Solaris 10 OS**. (October 2007. Glenn Brunette).
  - http://www.opensolaris.org/os/community/security/files/CEC-SFT0062-Brunette.pdf
- **Solaris 10 Security TOI - Deep Dive**. (September 2007. Glenn Brunette).
  - http://www.opensolaris.org/os/community/security/files/s10-security-dive-20070906.pdf
- **Practical Solaris 10 Security**. (October 2006, Glenn Brunette).
  - http://www.opensolaris.org/os/community/security/files/nsa-rebl-solaris.pdf

Attacker Goals

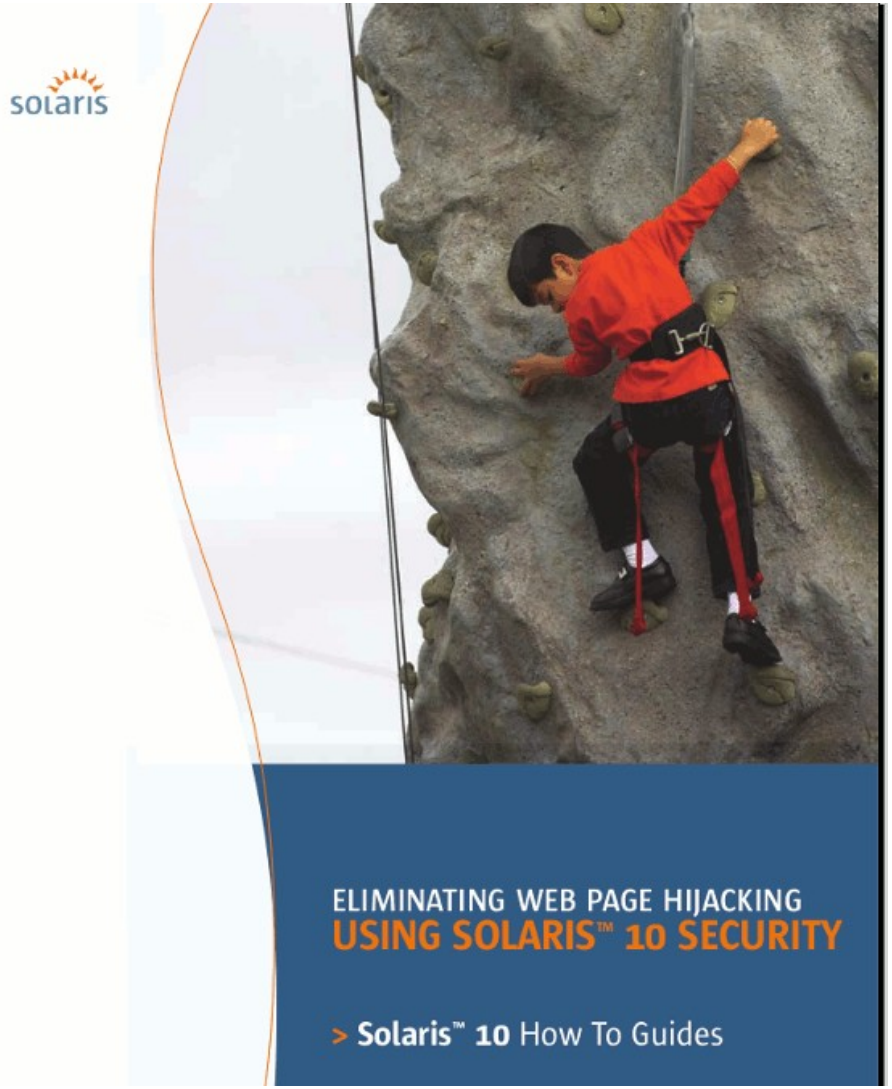
- Local System Access
- Administrative Privileges
- Access Privileged Information
- Conceal Attack and Avoid Detection
- Inject, Modify or Destroy Local Content
- Staging Platform for Further Attacks

Attack Scenario Background

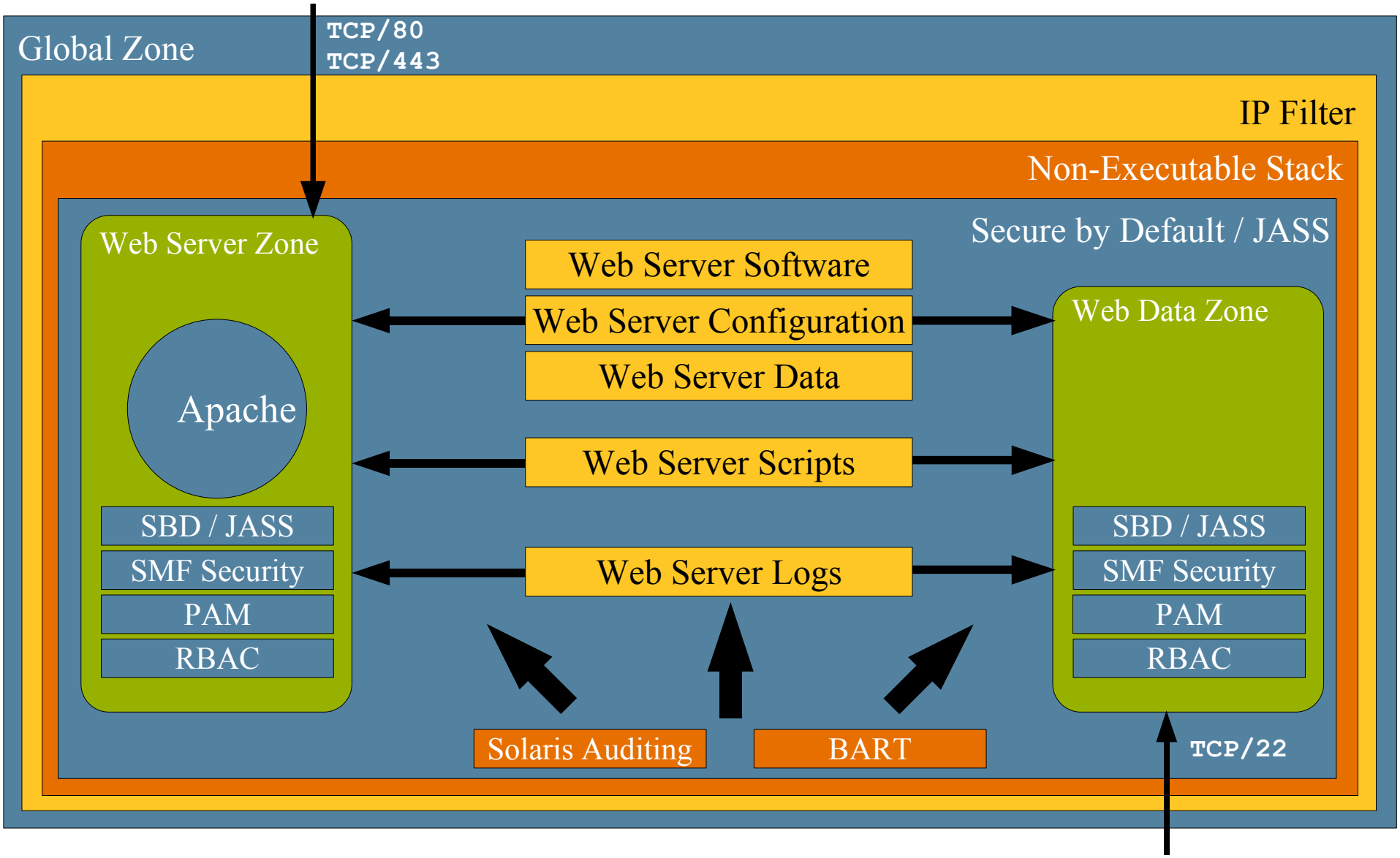
- While operating from the network
  - Our attack will originate from a local or remote network.
  - Our attacker does not have local system access (yet).
- While operating from the local system:
  - Our attacker has obtained unprivileged command line access (at least initially).
- In Both Cases:
  - All network services are offered from a Solaris sparse root zone.
  - Solaris global zone == "service processor"

http://www.sun.com/software/solaris/howtoguides/s10securityhowto.jsp

- The baseline for hardening the target system is taken from the How To Guide listed here.
- Technologies include: Zones, Secure By Default, SMF security, and Least Privilege



Target Environment Configuration



Service Enumeration Results w/IP Filter

```
# nmap -A webzone

Starting Nmap 4.20 ( http://insecure.org ) at 2008-04-12 16:59 BST
Warning: OS detection for webzone will be MUCH less reliable because we did
not find at least 1 open and 1 closed TCP port.
Interesting ports on webzone:
Not shown: 1695 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.2.8 ((Unix) mod_ssl/2.2.8
                                             OpenSSL/0.9.8a DAV/2 PHP/5.2.4)
443/tcp open  ssl/http Apache httpd 2.2.8 ((Unix) mod_ssl/2.2.8
                                             OpenSSL/0.9.8a DAV/2 PHP/5.2.4)
Device type: general purpose
Running: Sun Solaris 9|10
OS details: Sun Solaris 9 or 10

OS and Service detection performed. Please report any incorrect results at
http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 98.753 seconds
```

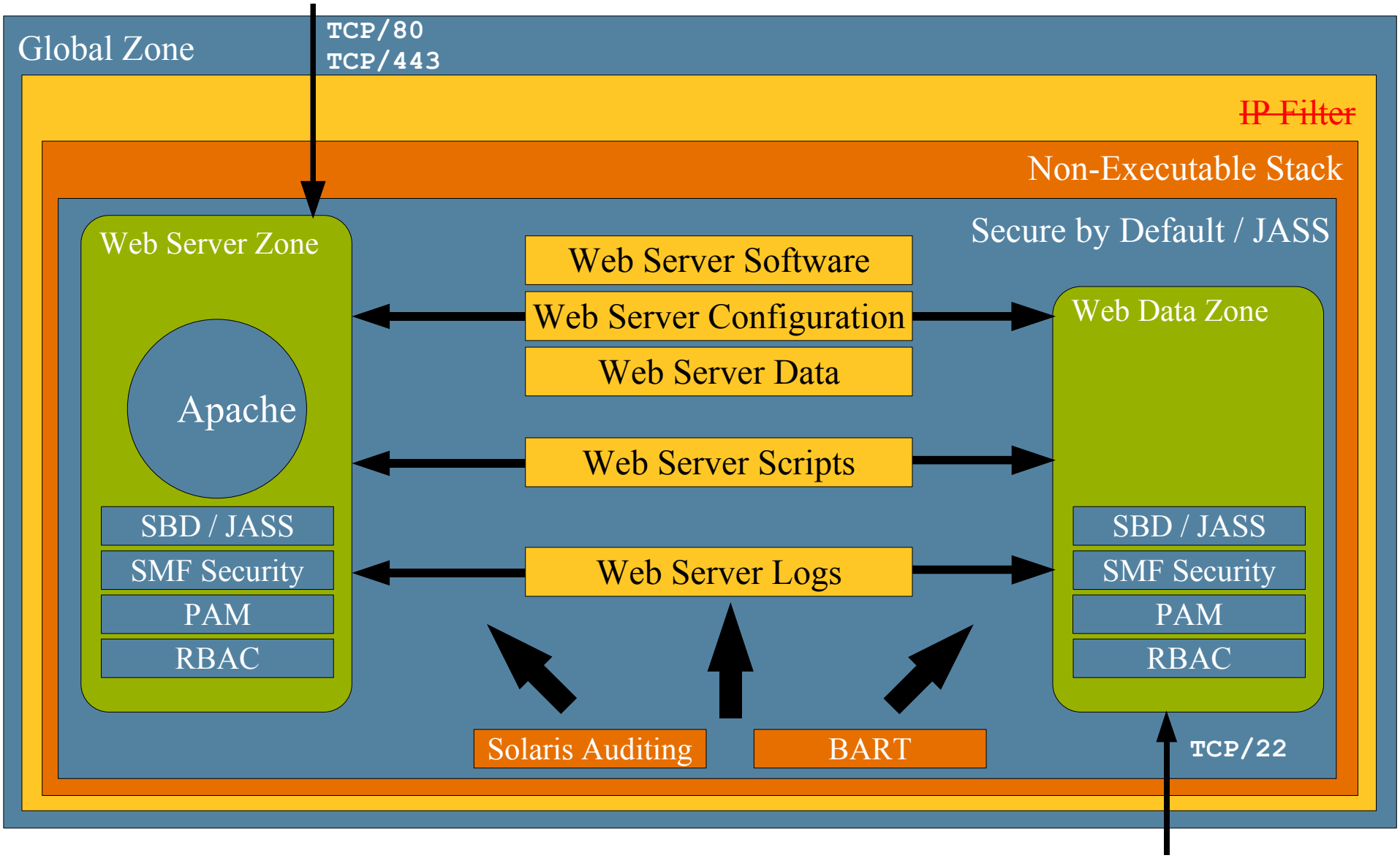
IP Filter Configuration

```
$ cat /etc/ipf/ipf.conf

set intercept_loopback true;

# *** GLOBAL ZONE: (IN: TCP/22, OUT: ANYTHING)
pass in quick proto tcp from any to global-zone port = 22
   keep state keep frags
pass out quick from global-zone to any keep state keep frags

# *** Web Server ZONE: (IN: TCP/80 + TCP/443, OUT: NOTHING)
pass in quick proto tcp from any to webzone port = 80
   keep state keep frags
pass in quick proto tcp from any to webzone port = 443
   keep state keep frags
block out quick from webzone to any

# *** Web Data ZONE: (IN: TCP/22, OUT: ANYTHING)
pass in quick proto tcp from any to datazone port = 22
   keep state keep frags
pass out quick from datazone to any keep state keep frags

# *** DEFAULT DENY
block in log all
block in from any to 255.255.255.255
block in from any to 127.0.0.1/32
```

Service Enumeration Results w/o IP Filter

```
# nmap -A webzone

Starting Nmap 4.20 ( http://insecure.org ) at 2008-04-12 20:49 BST
Interesting ports on webzone:
Not shown: 1693 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     SunSSH 1.1 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.2.8 ((Unix) mod_ssl/2.2.8
                                          OpenSSL/0.9.8a DAV/2 PHP/5.2.4)
111/tcp open  rpcbind  2-4 (rpc #100000)
443/tcp open  ssl/http Apache httpd 2.2.8 ((Unix) mod_ssl/2.2.8
                                          OpenSSL/0.9.8a DAV/2 PHP/5.2.4)
No exact OS matches for host (If you know what OS is running on it, see
  http://insecure.org/nmap/submit ).
Uptime: 0.186 days (since Sat Apr 12 16:42:35 2008)
Network Distance: 2 hop

OS and Service detection performed. Please report any incorrect
results at http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 1288.040 seconds
```

Target Environment Configuration



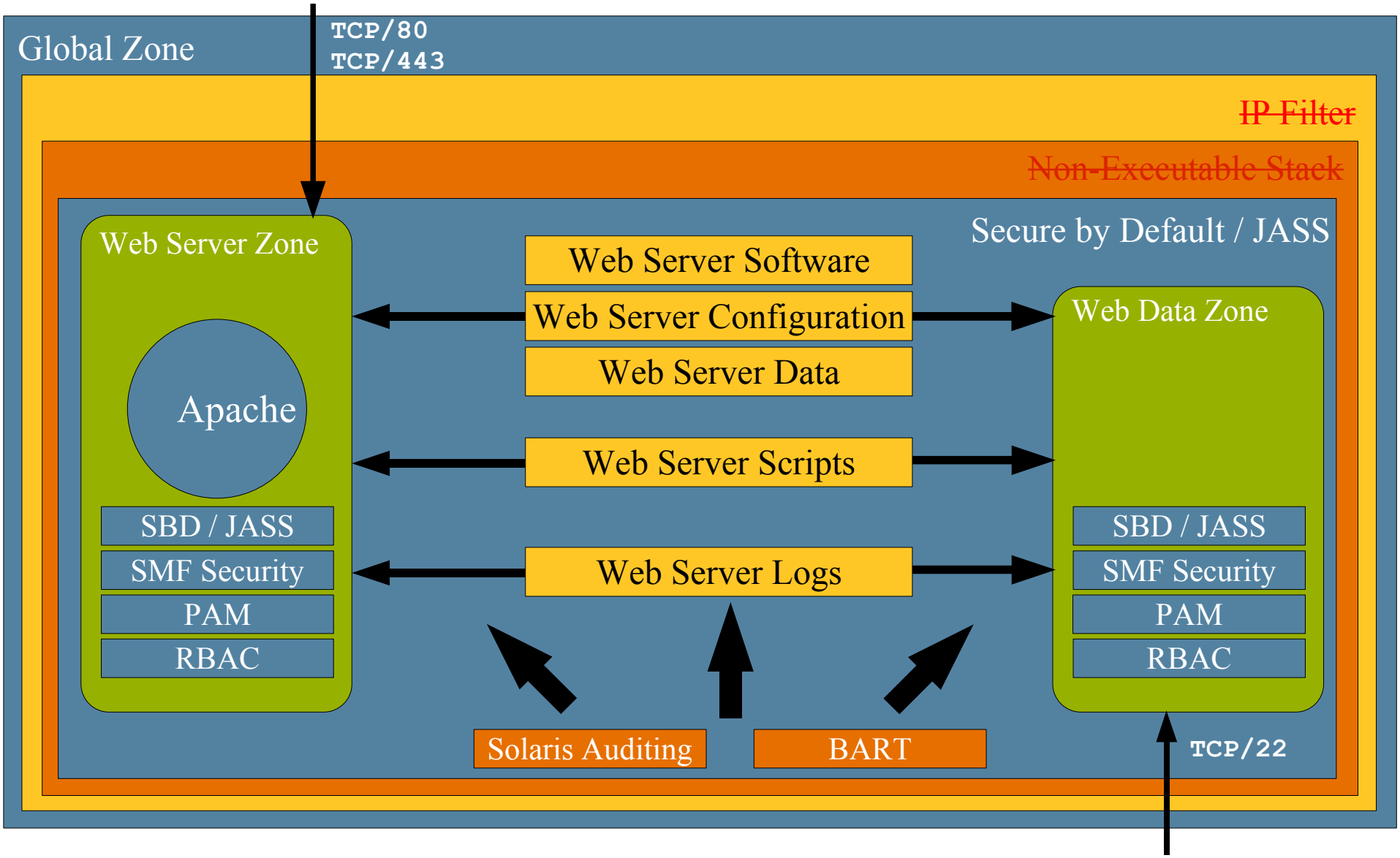
Executable Stacks and Security

```
$ cc -o shell-exstk shell.c
$ cc -o shell-noexstk -M /usr/lib/ld/map.noexst shell.c
OR
$ gcc -o shell-noexstk -Wl,-M/usr/lib/ld/map.noexstk shell.c
```

```
$ ./shell-exstk
Attempting to start a shell...
$ exit

$ ./shell-noexstk
Attempting to start a shell...
Segmentation Fault(coredump)

Apr 14 15:06:06 webzone genunix: [ID 533030 kern.notice]
NOTICE: shell-noexstk[23132] attempt to execute code on
stack by uid 101
```

Stacks can be globally configured to be non-executable using the noexec_user_stack kernel tunable in /etc/system.

Target Environment Configuration



Solaris Secure By Default Example

http://opensolaris.org/os/community/security/projects/sbd/

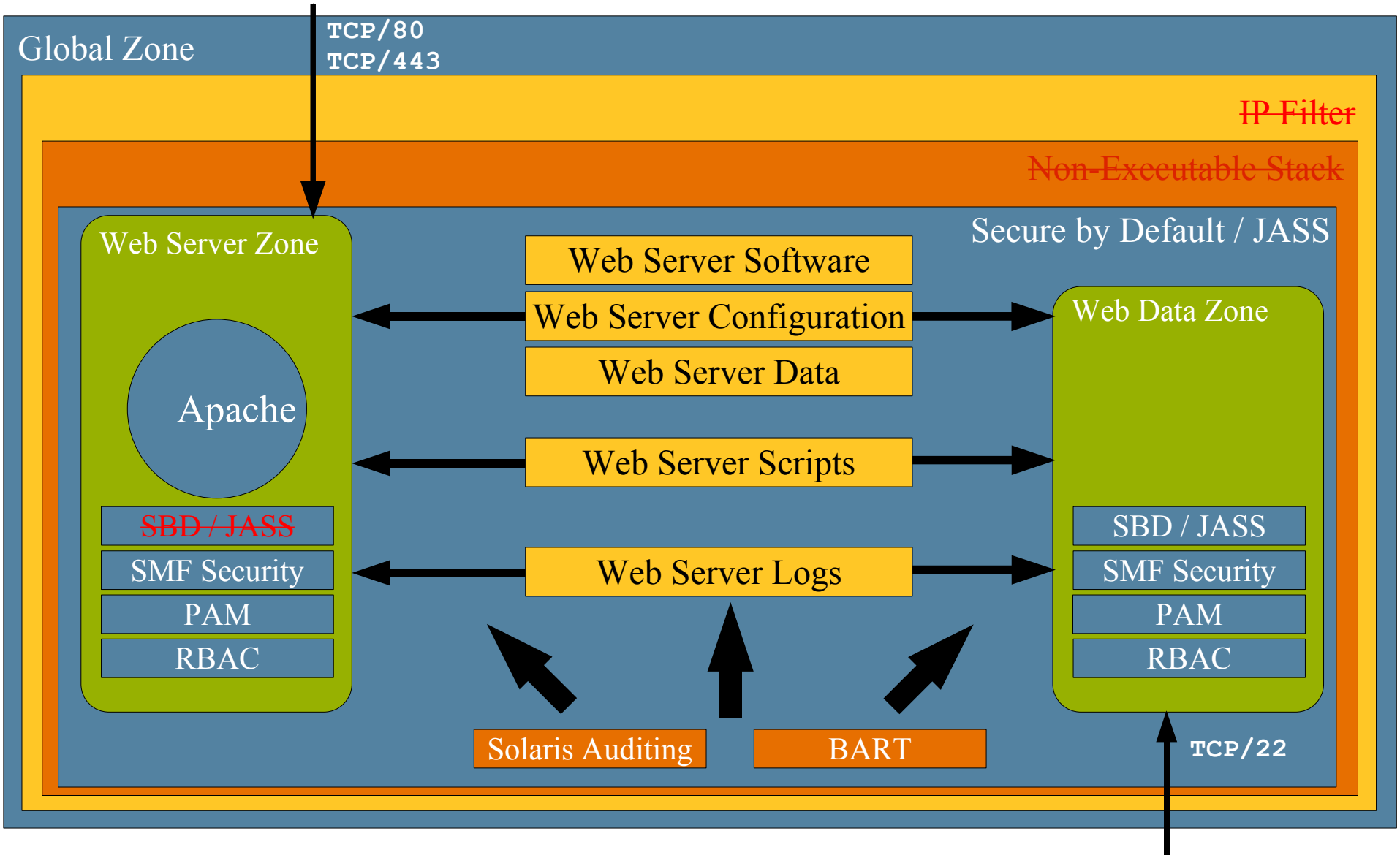
```
webzone# netservices open
webzone$ netstat -af inet | grep -c LISTEN
24
# nmap -A webzone

Starting Nmap 4.20 ( http://insecure.org ) at 2008-04-16 16:34 BST
Interesting ports on datazone (129.156.215.189):
Not shown: 1684 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Solaris ftpd
22/tcp    open  ssh           SunSSH 1.2 (protocol 2.0)
23/tcp    open  telnet        BSD-derived telnetd
25/tcp    open  smtp          Sendmail 8.14.2+Sun/8.14.2
79/tcp    open  finger        Sun Solaris fingerd
111/tcp   open  rpcbind        2-4 (rpc #100000)
513/tcp   open  rlogin
514/tcp   open  tcpwrapped
587/tcp   open  smtp          Sendmail 8.14.2+Sun/8.14.2
898/tcp   open  http          Solaris management console server (Java
1.6.0_04; Tomcat 2.1; SunOS 5.11 x86)
4045/tcp open  nlockmgr       1-4 (rpc #100021)
6112/tcp open  dtspc?
7100/tcp open  font-service Sun Solaris fs.auto
No exact OS matches for host (If you know what OS is running on it, see
http://insecure.org/nmap/submit/ ).
```

Solaris Secure By Default Example

http://opensolaris.org/os/community/security/projects/sbd/

```
webzone# netservices limited
webzone$ netstat -af inet
UDP: IPv4
   Local Address        Remote Address      State
-------------------- -------------------- ----------
      *.sunrpc                              Idle
      *.*                                   Unbound
      *.57610                               Idle
TCP: IPv4
   Local Address   Remote Address    Swind Send-Q Rwind Recv-Q State
   -------------   --------------    ----- ------ ----- ------ ------
      *.sunrpc        *.*                0      0 49152      0 LISTEN
      *.ssh           *.*                0      0 49152      0 LISTEN
localhost.smtp        *.*                0      0 49152      0 LISTEN
localhost.submission  *.*                0      0 49152      0 LISTEN
      *.80            *.*                0      0 49152      0 LISTEN
      *.443           *.*                0      0 49152      0 LISTEN
```

Target Environment Configuration



SMF Method Context Example

Original Apache2.2 SMF start method:

```
$ svcprop -v -p start apache22
start/exec astring /lib/svc/method/http-apache2\ start
start/timeout_seconds count 60
start/type astring method
```

After modification using svccfg(1M):

```
$ svcprop -v -p start apache22
start/exec astring /lib/svc/method/http-apache2\ start
start/timeout_seconds count 60
start/type astring method
start/user astring webservd
start/group astring webservd
start/privileges astring
basic,!proc_session,!proc_info,!file_link_any,net_privaddr
start/limit_privileges astring :default
start/use_profile boolean false
start/supp_groups astring :default
start/working_directory astring :default
start/project astring webproj
start/resource_pool astring :default
```

Fine Grained Access Policy (FGAP)

http://opensolaris.org/os/project/fgap/

"This project will extend the existing Process Rights Management infrastructure in Solaris so that specified objects can be associated with individual privileges. The current Solaris privilege model does not allow one to express policy requirements such as:

- only allow binding to port 80/tcp

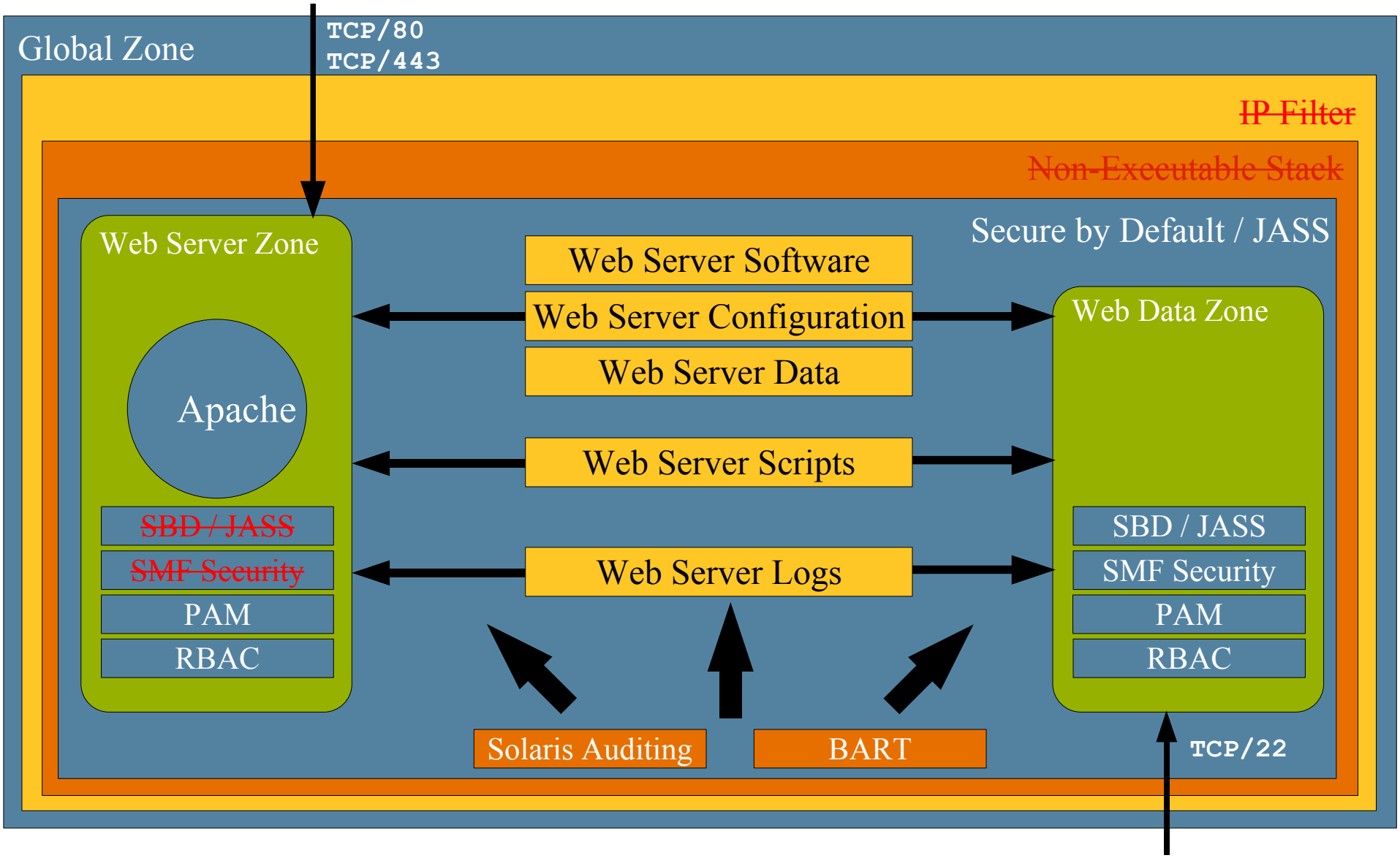
- only allow read access to file foo

- only allow write access under $HOME/.mozilla

"

```
Currently the net_privaddr privilege applies to all privileged ports:

$ ppriv -v -l net_privaddr
net_privaddr
        Allows a process to bind to a privileged port
        number. The privilege port numbers are 1-1023 (the traditional
        UNIX privileged ports) as well as those ports marked as
        "udp/tcp_extra_priv_ports" with the exception of the ports
        reserved for use by NFS.
```

Target Environment Configuration



PAM User/Password Controls

- Pluggable Crypt - /etc/security/{policy,crypt}.conf
  - Sun MD5 (+ rounds), BSD MD5, Blowfish
- Password Complexity Checks - authtok_check.c
  - Login Name != Password, White Space Permitted?
  - Minimum Characters by Class
    - Alphabetic, Non-Alphabetic, Uppercase, Lowercase, Digits, Punctuation
  - Maximum Consecutive Repeating Characters
  - Local Banned Password List (Dictionary)
- Password Aging and History
- Account Lockout (local accounts only)

Pluggable Crypt Example

```
$ grep "^CRYPT_DEFAULT=" /etc/security/policy.conf
CRYPT_DEFAULT=md5

$ grep "^md5" /etc/security/crypt.conf
md5     crypt_sunmd5.so.1 rounds=8000

# grep "^root" /etc/shadow
root:$md5,rounds=8000$kS9FT1JC$$mnUrRO618lLah5iazwJ9m1:13776::::::
```

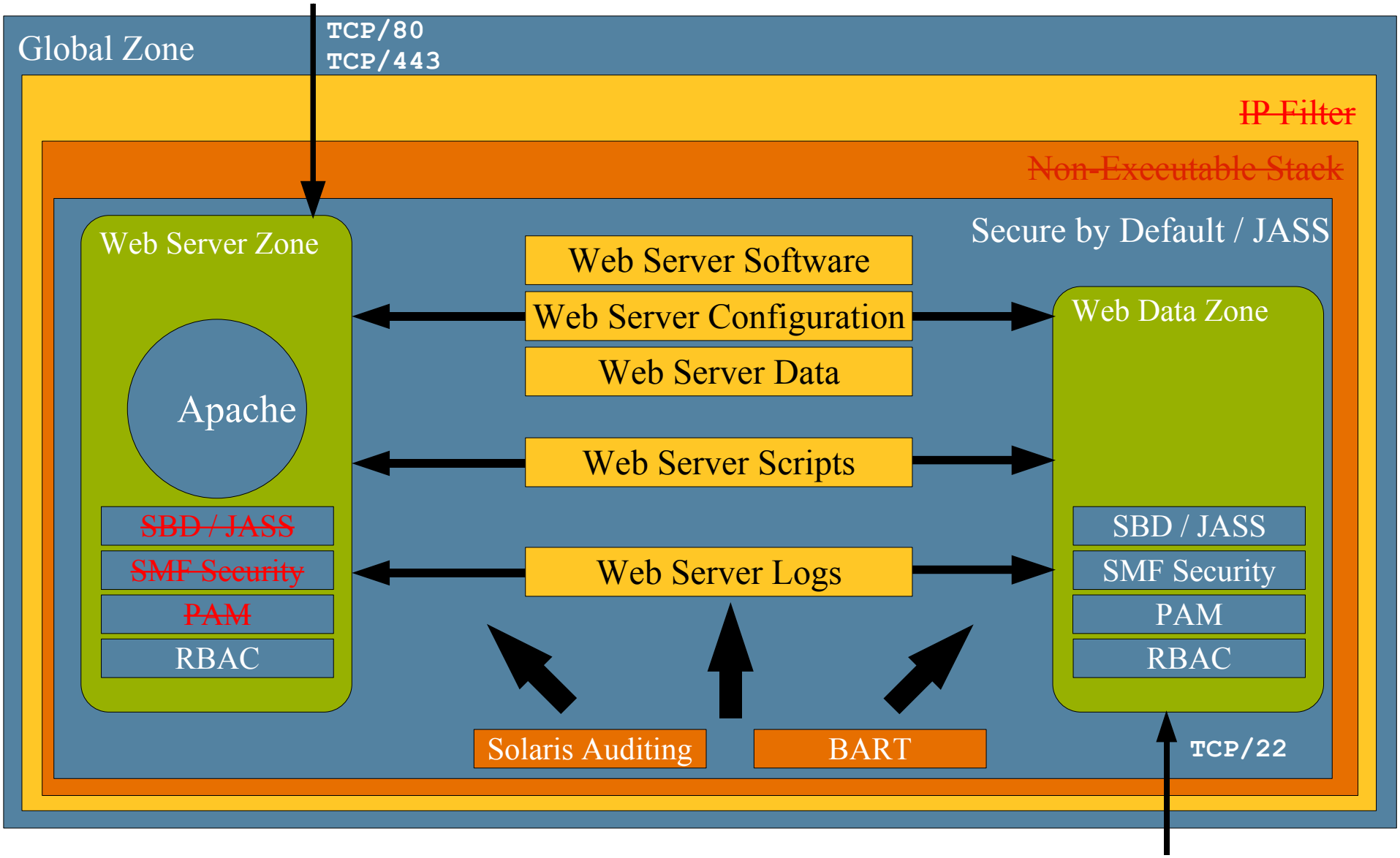
John the Ripper – http://en.wikipedia.org/wiki/John_the_Ripper

```
$ john ./mypasswd
No password hashes loaded
```

Crack – http://en.wikipedia.org/wiki/Crack_(software)

```
$ Crack ./mypasswd
$ Reporter | grep -w root
E:1190747899:StoreDataHook: invalid ciphertext: root
  $md5,rounds=8000$kS9FT1JC$$mnUsRO618lLah5iazwJ9m1
```

Target Environment Configuration



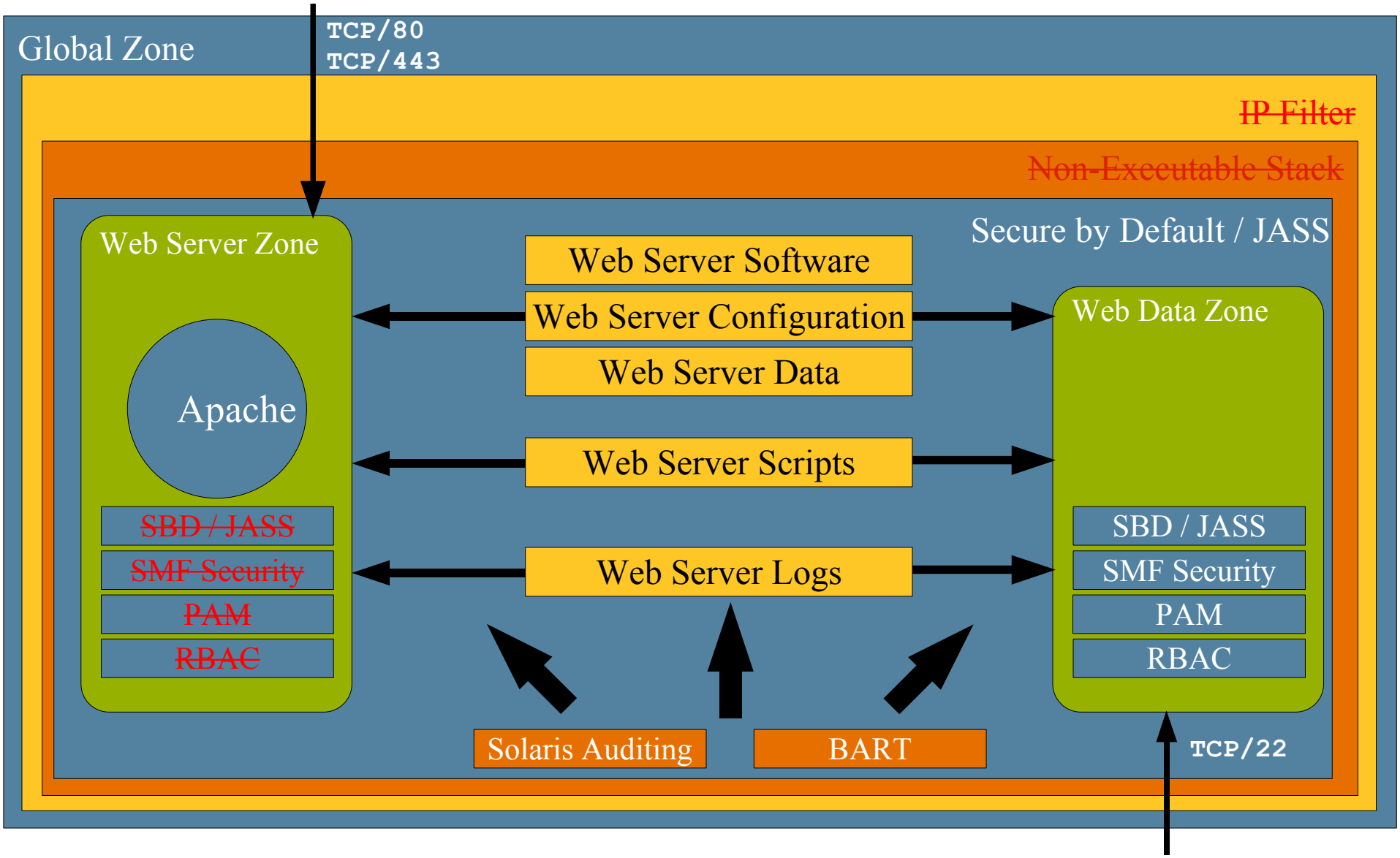
RBAC Configuration for webop user

```
webzone# profiles -l webop

      Web Server Operator:
          /usr/bin/svcs    privs=basic,!proc_exec,!file_link_any
          /usr/sbin/svcadm
          /opt/web/show_log
          /opt/web/show_errors

webzone# auths webop
solaris.smf.manage.http/apache22

webzone$ svcprop -p httpd -p general apache22
general/action_authorization astring solaris.smf.manage.http/apache22
general/enabled boolean false
general/value_authorization astring solaris.smf.value.http/apache22
general/entity_stability astring Evolving
httpd/enable_64bit boolean false
httpd/server_type astring prefork
httpd/stability astring Evolving
httpd/startup_options astring ""
httpd/value_authorization astring solaris.smf.value.http/apache22
```

RBAC command restrictions for webop

```
$ ssh webzone -l webop
Password:
Last login: Mon Apr 14 20:49:57 2008 from enoexec.uk.sun.com

$ ls
ls: not found
$ ps -aef
ps: not found
$ echo $SHELL
/bin/pfsh
$ /bin/sh
/bin/sh: not found
$ svcs apache22
STATE          STIME    FMRI
online         18:39:59 svc:/network/http:apache22
$ svcadm restart apache22
$ svcs apache22
STATE          STIME    FMRI
online         20:51:33 svc:/network/http:apache22
$ svcadm restart ssh
svcadm: svc:/network/ssh:default: Permission denied.
```

Target Environment Configuration



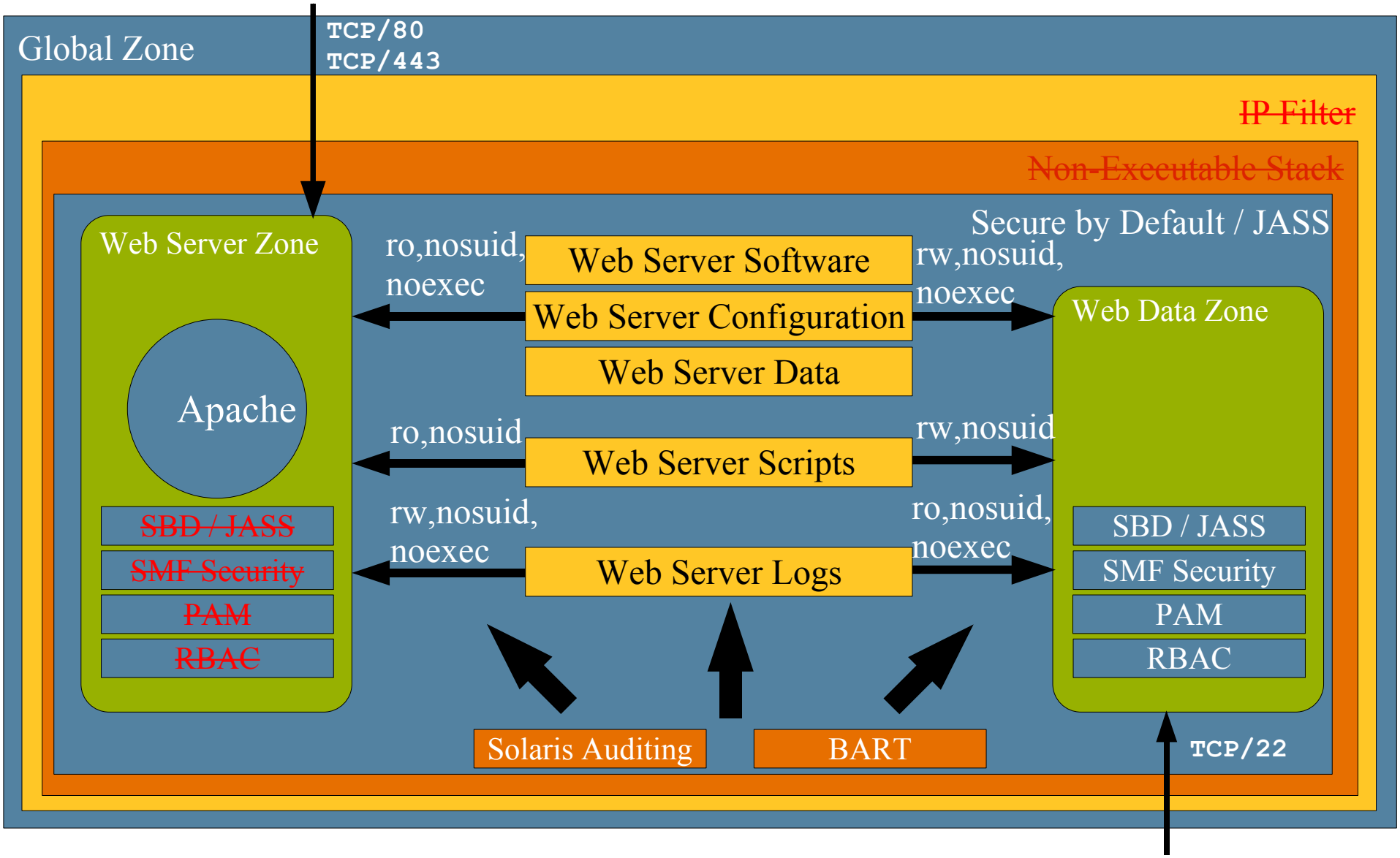
Why run services in Zones?

- Restricted Operations for Enhanced Security
  - Individual Solaris OS hardening and RBAC configurations.
  - Prohibited from directly accessing the kernel or raw memory.
  - Prohibited from manipulating network interfaces and kernel modules.
- Enforcement with Integrity
  - Configurable privileges, sparse root zones, IP Instances, IP Filter, etc.
- Observability with Integrity
  - BART, Solaris Auditing, etc.
- Resource Control and Management
  - CPU, Memory, Disk, Networking, Devices, etc.

Web Server Zone Configuration

```
$ zonecfg -z webzone info
[...]
fs:
        dir: /etc/apache2/2.2
        special: /z/shared/config
        type: lofs
        options: [ro,nodevices,nosuid,noexec]
fs:
        dir: /var/apache2/2.2/run
        special: /z/shared/run
        type: lofs
        options: [rw,nodevices,nosuid,noexec]
fs:
        dir: /var/apache2/2.2
        special: /z/shared/data
        type: lofs
        options: [ro,nodevices,nosuid,noexec]
fs:
        dir: /var/apache2/2.2/logs
        special: /z/shared/logs
        type: lofs
        options: [rw,nodevices,nosuid,noexec]
```

Target Environment Configuration



Zones Security Example #1

```
# cd /etc/apache2/2.2
# mv httpd.conf httpd.conf.orig
mv: cannot rename httpd.conf to httpd.conf.orig: Read-only file system

# cd /lib/svc/method
# mv http-apache22 http-apache22.orig
mv: cannot rename http-apache22 to http-apache22.orig: Read-only file
  system

# cd /usr/apache2/2.2/bin
# mv apachectl apachtctl.orig
mv: cannot rename apachectl to apachtctl.orig: Read-only file system

# cd /usr/bin
# mv login login.orig
mv: cannot rename login to login.orig: Read-only file system

$ mount -p
/ - / ufs - no rw,intr,largefiles,logging,xattr,onerror=panic
/dev - /dev dev - no
/lib - /lib lofs - no ro,nodevices,nosub
/platform - /platform lofs - no ro,nodevices,nosub
/sbin - /sbin lofs - no ro,nodevices,nosub
/usr - /usr lofs - no ro,nodevices,nosub
[...]
```

Zones Security Example #2

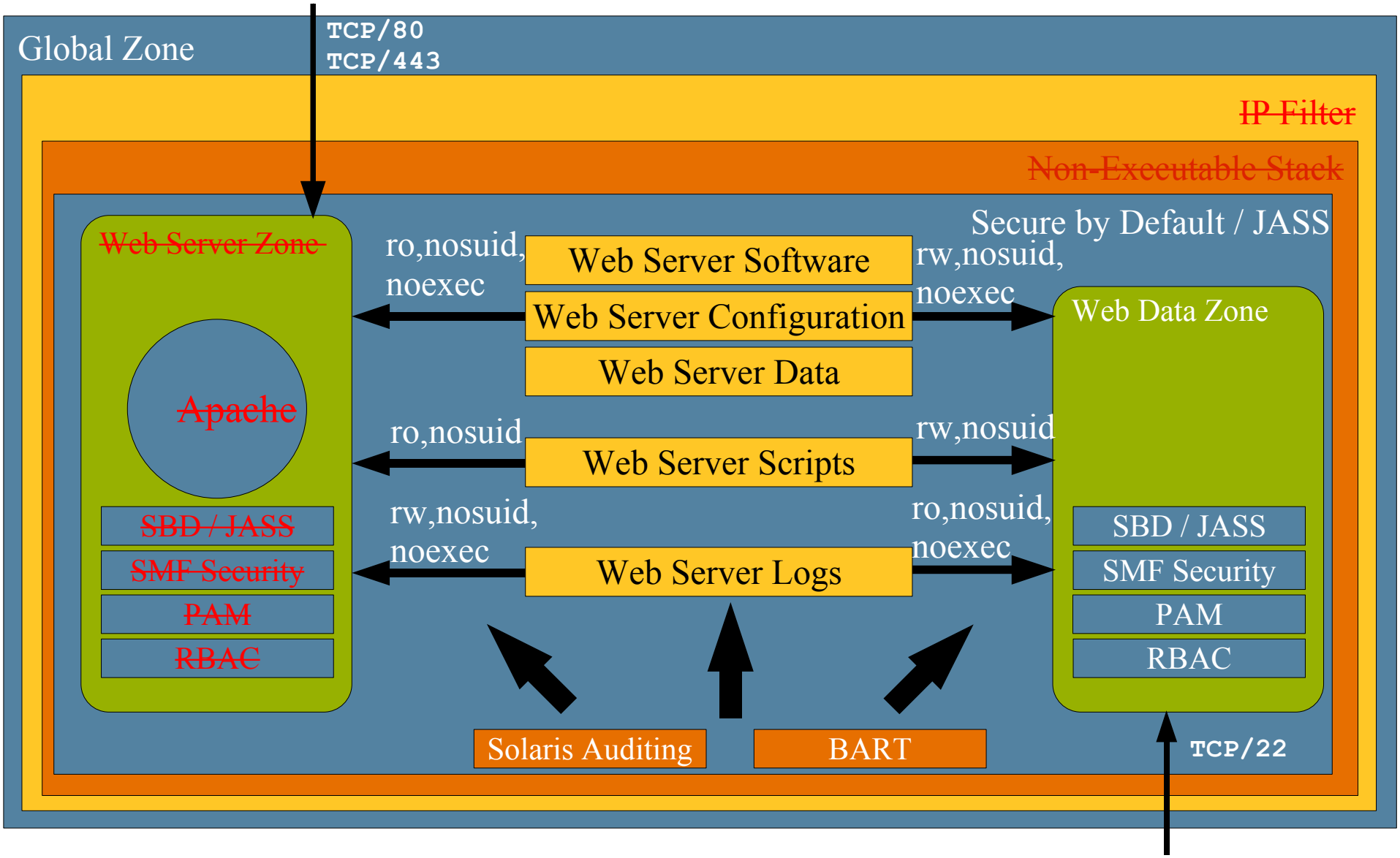
```
# modload drv/mymodule
Insufficient privileges to load a module

# modunload -i 101
Insufficient privileges to unload a module

# snoop
snoop: No network interface devices found

# mdb -k
mdb: failed to open /dev/ksyms: No such file or directory

# dtrace -l
   ID   PROVIDER            MODULE                          FUNCTION NAME

# ppriv -D -e route add net default 10.1.2.3
route[3633]: missing privilege "sys_ip_config" (euid = 0, syscall = 4)
  needed at secpolicy_ip_config+0x43
add net default: gateway 10.1.2.3: insufficient privileges
```

Zones Security Example with ZFS ACLs

ZFS ACLs can be used to restrict what commands can be executed in the global or a non-global zone.

```
globalzone# chmod A+user:webservd:execute:deny /z/zones/pop-tart/root/usr/bin/su

webzone$ id -a
uid=80(webservd) gid=80(webservd) groups=80(webservd)

webzone$ /usr/bin/su
/usr/bin/su: cannot execute

webzone$ ls -l /usr/bin/su
-r-sr-xr-x+  1 root     sys        34788 Mar 23 18:39 /usr/bin/su

webzone$ ls -v /usr/bin/su
-r-sr-xr-x+  1 root     sys        34788 Mar 23 18:39 /usr/bin/su
     0:user:webservd:execute:deny
     1:owner@:write_data/append_data:deny
     2:owner@:read_data/write_xattr/execute/write_attributes/write_acl
         /write_owner:allow
     [...]
```

Target Environment Configuration



Basic Audit Reporting Tool (BART)

File-level integrity validation tool:

- Evalutes: uid, gid, permissions/acls, contents, mtime, size, type, etc.

```
# find /etc | bart create -I > newManifest
# bart compare ./oldManifest ./newManifest

/etc/shadow:
  size  control:594  test:641
  mtime  control:46f959eb  test:46f95aeb
  contents  control:a665e97036c3284a6100438f092e97f0
     test:9d68e5ac60e00a19dea79be7b896133c
```

See: Sun BluePrint: Automating File Integrity Checks, http://www.sun.com/blueprints/0305/819-2259.pdf

Solaris Auditing

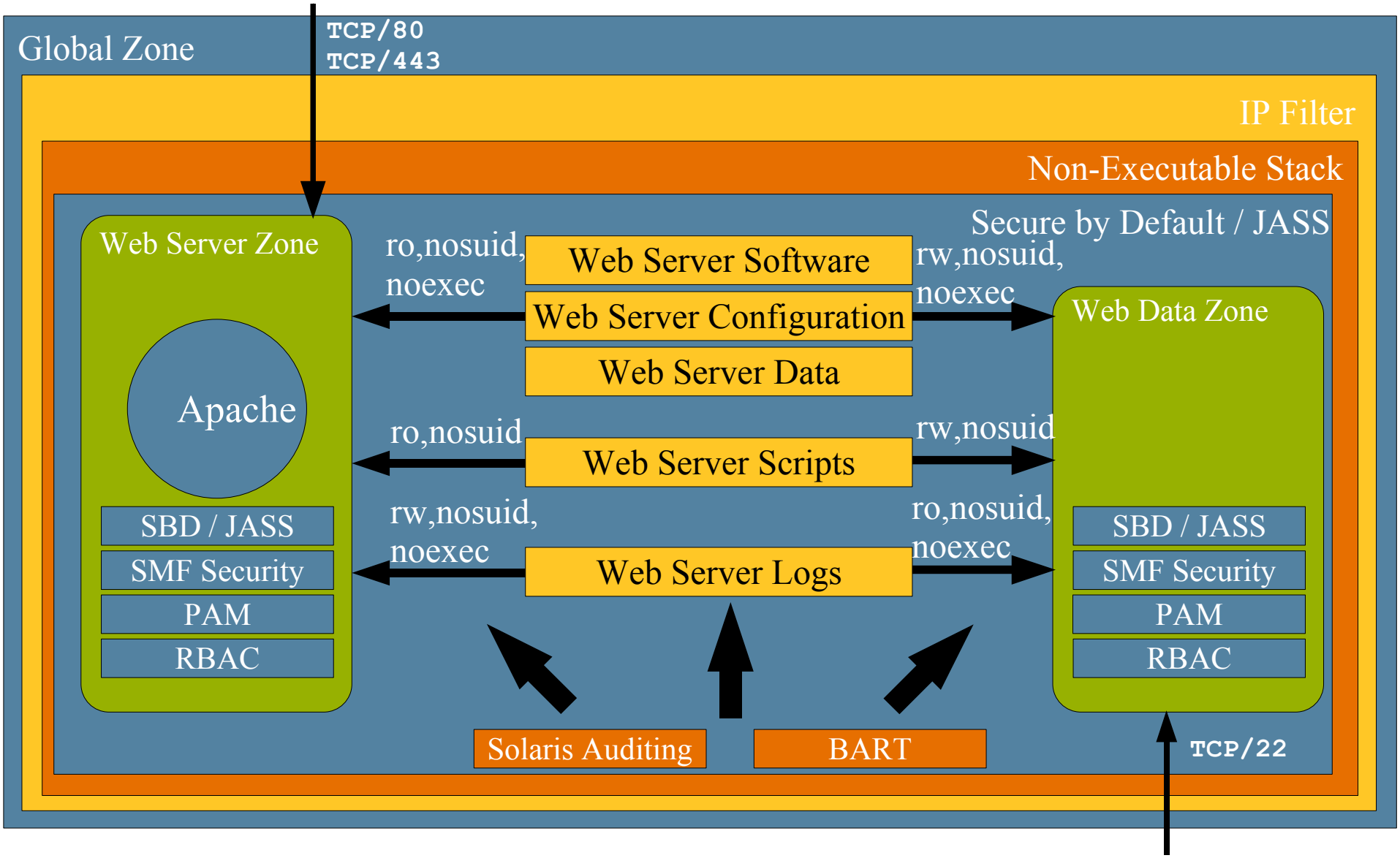
Kernel auditing of system calls and administrative actions.

> Can record events happening in any zone (from the global zone).

Example:

```
webzone$ id -a
uid=80(webservd) gid=80(webservd) groups=80(webservd)

webzone$ su
Password:
su: Sorry

globalzone# auditreduce -z webzone -m AUE_su | praudit
header,88,2,su,,va64-x2100d-gmp03,2008-04-15 13:26:23.842 +01:00
subject,webservd,root,webservd,webservd,webservd,9126,3698614514,164 3 webzone
text,root
return,failure,Authentication failed
zone,webzone
```

Target Environment Configuration



Attacker Goals

- Local System Access
- Administrative Privileges
- Access Privileged Information
- Conceal Attack and Avoid Detection
- Inject, Modify or Destroy Local Content
- Staging Platform for Further Attacks

Additional Controls Not Covered

- Operating System Minimization (e.g. SUNWCrnet)
- TCP Wrappers
- Signed ELF Objects (elfsign(1))
- Solaris Fingerprint Database
  - http://opensolaris.org/os/project/forensics/Tools/sfpdb-tools/
- Validated Execution Project
  - http://opensolaris.org/os/project/valex/
- Solaris Trusted Extensions
  - http://opensolaris.org/os/community/security/projects/tx/
- Solaris Cryptographic Framework
  - http://opensolaris.org/os/project/crypto/
- Kerberos
  - http://opensolaris.org/os/project/kerberos/

For More Information

- Sun Security Home
  - http://www.sun.com/security
- OpenSolaris Security Community
  - http://www.opensolaris.org/os/community/security
- Sun Security Coordination Center
  - http://blogs.sun.com/security & security-alert@sun.com
- Sun Security BluePrints
  - http://www.sun.com/security/blueprints

開
放
的
열린
مفتوح
libre
मुक्त
ಮುಕ್ತ
livre
libero
ముక్త
开放的
açık
open
nyílt
פתוח
オープン
livre
ανοικτό
offen
otevřený
öppen
открытый
வெளிப்படை

open

USE IMPROVE EVANGELIZE

Thank you!

Brent Paulson
Solaris Sustaining
Sun Microsystems, Inc.

“open” artwork and icons by chandan:
http://blogs.sun.com/chandan