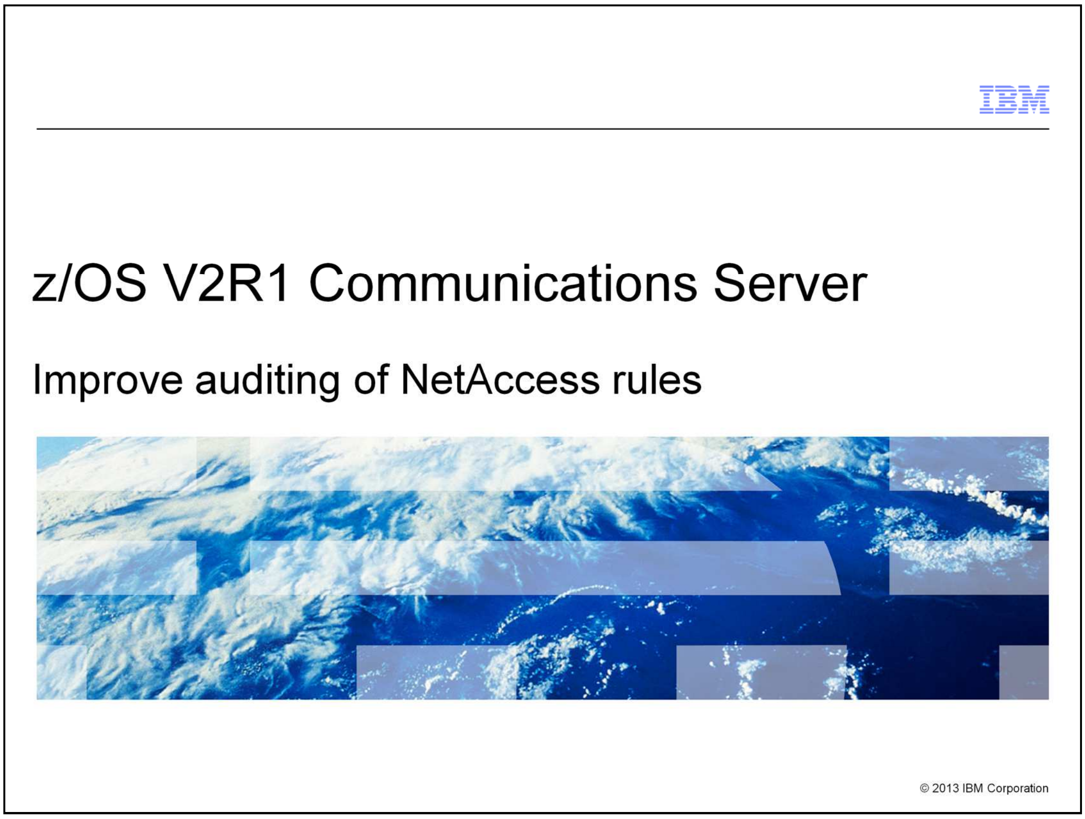
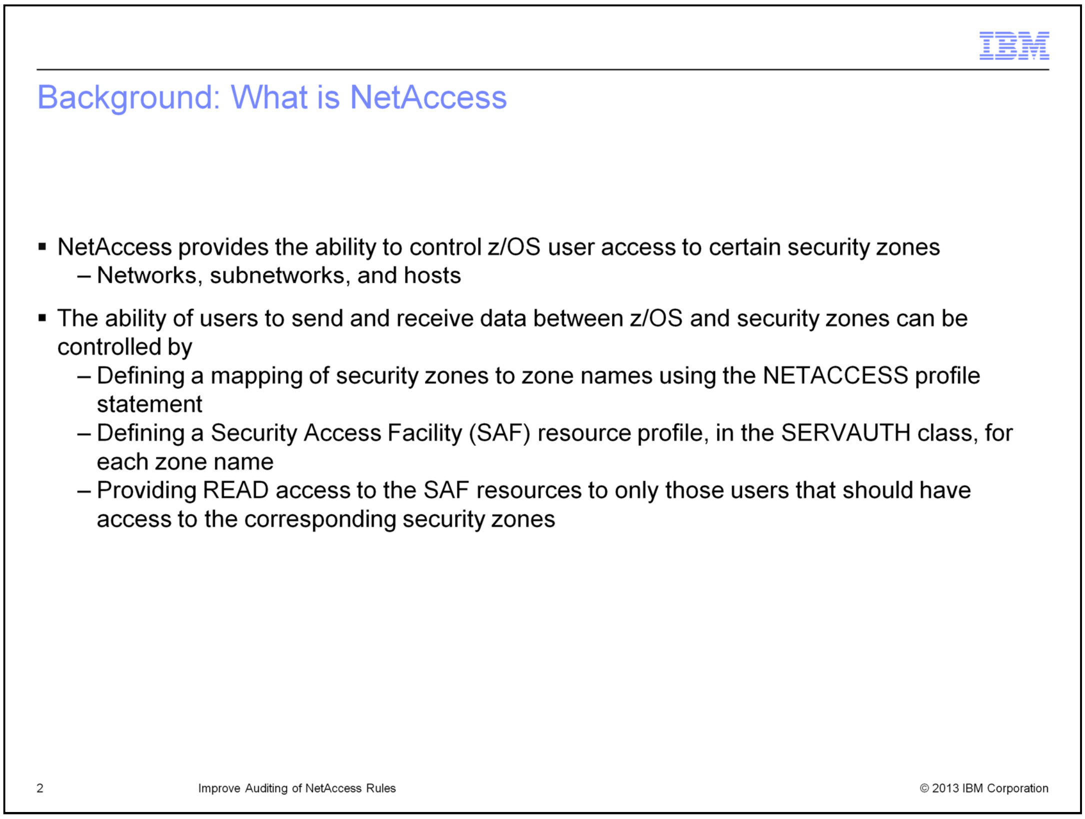


z/OS V2R1 Communications Server

Improve auditing of NetAccess rules

This presentation covers the changes made in z/OS® V2R1 Communications Sever to improve auditing of NetAccess rules.



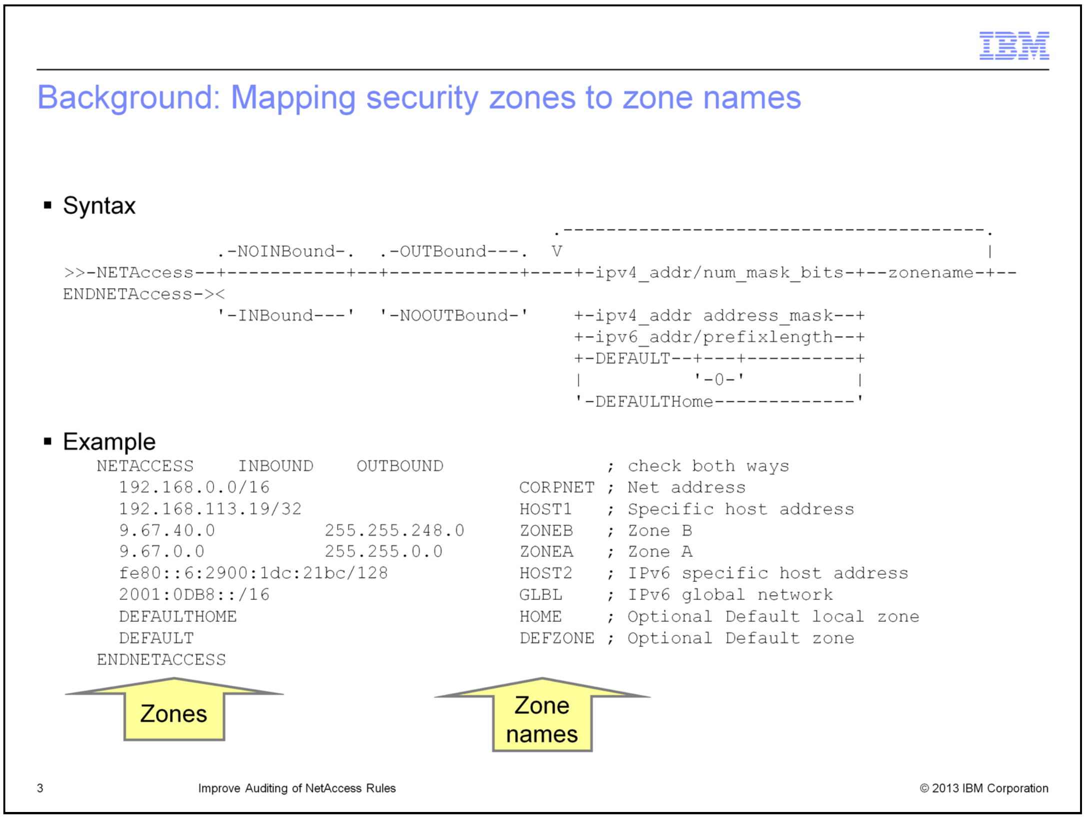
Background: What is NetAccess

- NetAccess provides the ability to control z/OS user access to certain security zones
  - Networks, subnetworks, and hosts
- The ability of users to send and receive data between z/OS and security zones can be controlled by
  - Defining a mapping of security zones to zone names using the NETACCESS profile statement
  - Defining a Security Access Facility (SAF) resource profile, in the SERVAUTH class, for each zone name
  - Providing READ access to the SAF resources to only those users that should have access to the corresponding security zones

NetAccess, or Network Access, is the Communications Server function that provides a system programmer with the ability to control user access to networks, subnetworks, and hosts. These networks, subnetworks, and hosts are referred to as security zones and access to the security zones by individual users can be either permitted or not permitted using NetAccess.

User access to a security zone determines user’s ability to send and receive data between z/OS and the IP addresses in the zone.

There are three setup steps needed to control access to security zones. First, the NETACCESS statement in the TCP/IP profile is configured to define a mapping of security zones to zone names. Next, Security Access Facility resource profiles are defined, in the SERVAUTH class, for each zone name. Finally, read access to the Security Access Facility resource profiles is provided to only those users that should have access to the corresponding security zones.



Background: Mapping security zones to zone names

- Syntax

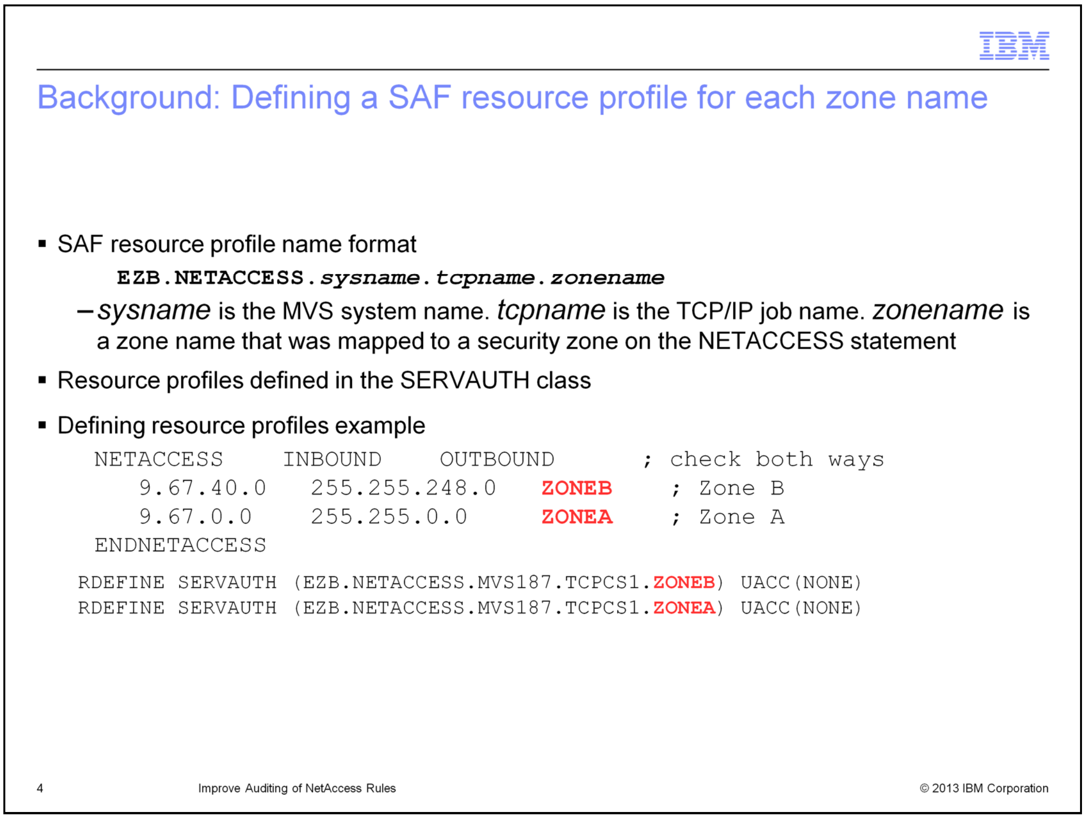
```
                                              .--------------------------------------.
              .-NOINBound-.  .-OUTBound---.   V                                      |
>>-NETAccess--+-----------+--+------------+----+-ipv4_addr/num_mask_bits-+--zonename-+--
ENDNETAccess-><
              '-INBound---'  '-NOOUTBound-'    +-ipv4_addr address_mask--+
                                               +-ipv6_addr/prefixlength--+
                                               +-DEFAULT--+---+----------+
                                               |          '-0-'          |
                                               '-DEFAULTHome-------------'
```

- Example

```
   NETACCESS    INBOUND    OUTBOUND               ; check both ways
     192.168.0.0/16                       CORPNET ; Net address
     192.168.113.19/32                    HOST1   ; Specific host address
     9.67.40.0          255.255.248.0     ZONEB   ; Zone B
     9.67.0.0           255.255.0.0       ZONEA   ; Zone A
     fe80::6:2900:1dc:21bc/128            HOST2   ; IPv6 specific host address
     2001:0DB8::/16                       GLBL    ; IPv6 global network
     DEFAULTHOME                          HOME    ; Optional Default local zone
     DEFAULT                              DEFZONE ; Optional Default zone
   ENDNETACCESS
```

The NETACCESS statement in the TCP/IP profile is used to define a mapping of security zones to zone names. The purpose of this mapping is to provide a name for each security zone so the names can then be used in the Security Access Facility resource profile names that are defined in the next step.

The syntax of the configuration statement is shown here along with an example of the statement that defines the mapping of eight security zones to zone names. In the example you can see that the security zones are subsets of IP addresses. Zones are specified as entire networks, subnetworks, or single IP addresses. Both IPv4 and IPv6 addresses can be specified. The DEFAULT and DEFAULTHOME entries define the zone names for networks that are not specifically defined by other entries.



Background: Defining a SAF resource profile for each zone name

- SAF resource profile name format

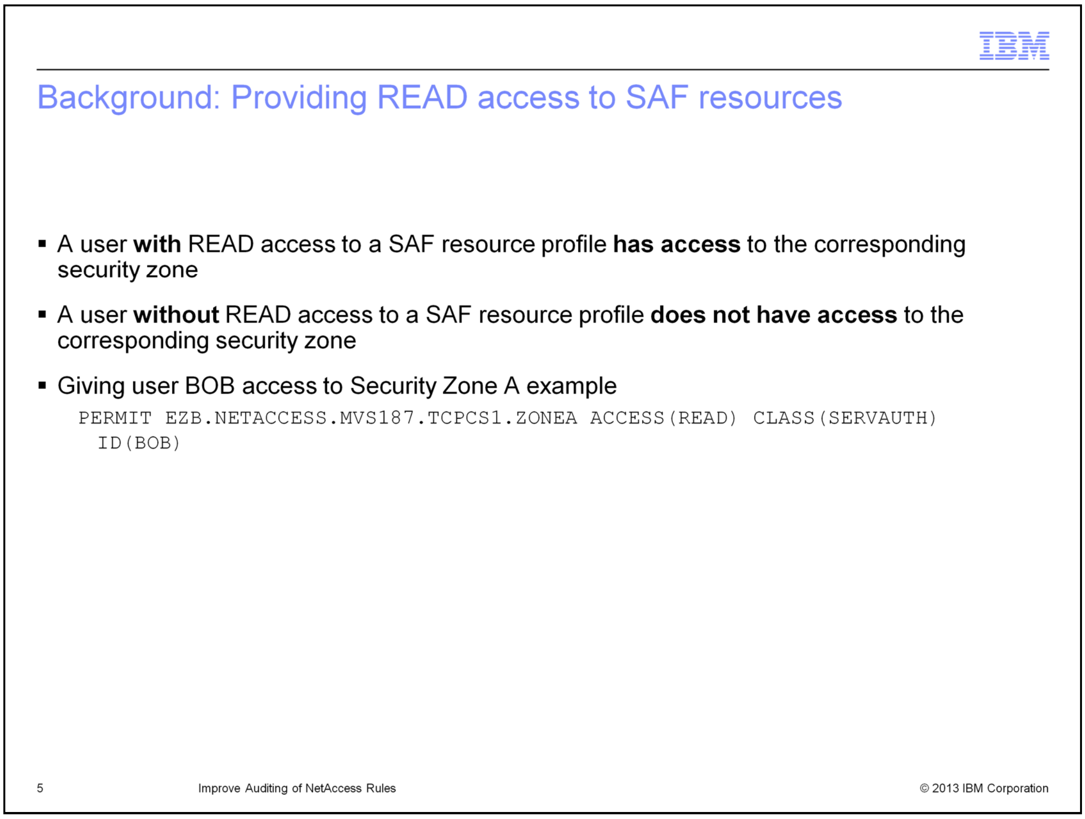
  EZB.NETACCESS.*sysname*.*tcpname*.*zonename*

  – *sysname* is the MVS system name. *tcpname* is the TCP/IP job name. *zonename* is a zone name that was mapped to a security zone on the NETACCESS statement
- Resource profiles defined in the SERVAUTH class
- Defining resource profiles example

```
NETACCESS     INBOUND     OUTBOUND       ; check both ways
   9.67.40.0    255.255.248.0    ZONEB     ; Zone B
   9.67.0.0     255.255.0.0      ZONEA     ; Zone A
ENDNETACCESS

RDEFINE SERVAUTH (EZB.NETACCESS.MVS187.TCPCS1.ZONEB) UACC(NONE)
RDEFINE SERVAUTH (EZB.NETACCESS.MVS187.TCPCS1.ZONEA) UACC(NONE)
```

After zone names are defined for each security zone, Security Access Facility resource profiles can be defined for each name. The resource profiles are defined in the SERVAUTH class.

The format of the resource profile names used for NetAccess is shown, along with an example. The example shows a NETACCESS profile statement that defines the mapping of two security zones to their security names. That is followed by the RACF® RDEFINE statements that define Security Access Facility resource profiles for the two security zones. The UACC(NONE) parameter on the RDEFINE statement indicates that users are denied access to the resource unless access is explicitly granted.



Background: Providing READ access to SAF resources

- A user **with** READ access to a SAF resource profile **has access** to the corresponding security zone
- A user **without** READ access to a SAF resource profile **does not have access** to the corresponding security zone
- Giving user BOB access to Security Zone A example

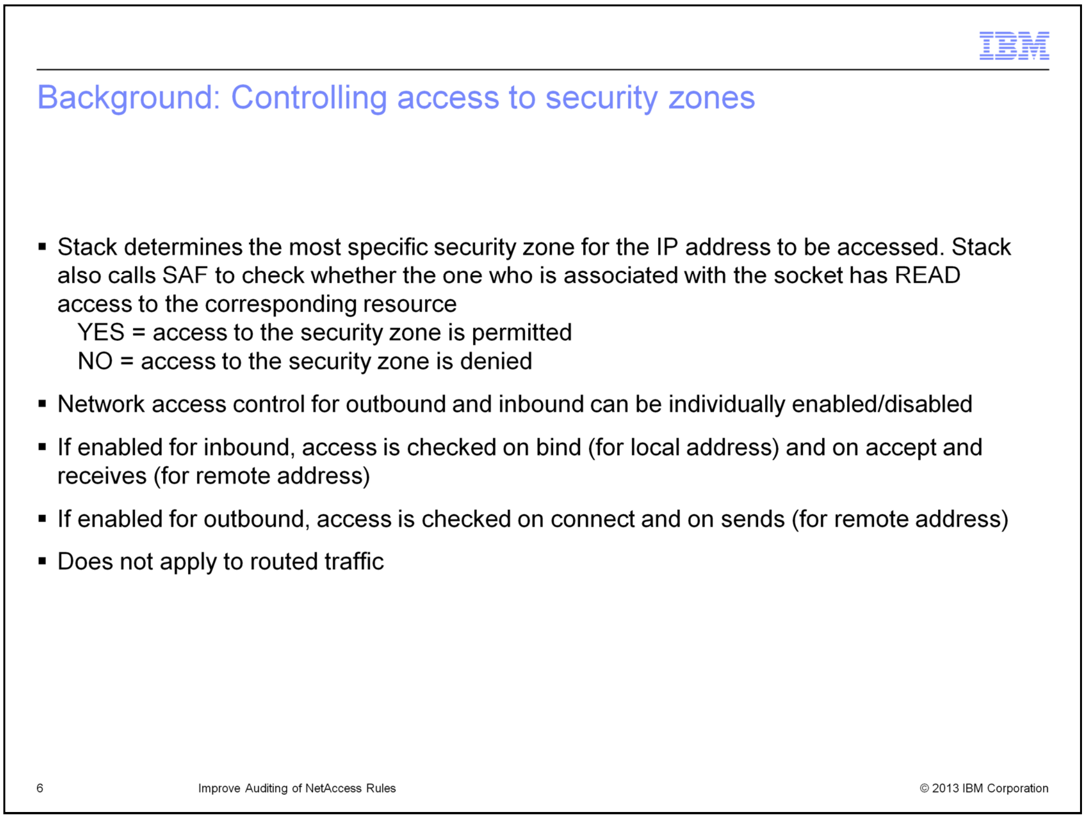
```
PERMIT EZB.NETACCESS.MVS187.TCPCS1.ZONEA ACCESS(READ) CLASS(SERVAUTH)
  ID(BOB)
```

5 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

With the Security Access Facility resource profiles defined for each zone name, the final step can be completed. This step grants individual users read access to the Security Access Facility resource profiles.

Each user who is given read access to a particular resource profile will have access to the corresponding security zone. All other users will not have access to that security zone.

The example shows the RACF PERMIT statement that is issued to give user BOB access to the security zone with the name ZONEA. If this is the only PERMIT statement issued for the zone, no other users will have access to the zone.



Background: Controlling access to security zones

- Stack determines the most specific security zone for the IP address to be accessed. Stack also calls SAF to check whether the one who is associated with the socket has READ access to the corresponding resource
  YES = access to the security zone is permitted
  NO = access to the security zone is denied
- Network access control for outbound and inbound can be individually enabled/disabled
- If enabled for inbound, access is checked on bind (for local address) and on accept and receives (for remote address)
- If enabled for outbound, access is checked on connect and on sends (for remote address)
- Does not apply to routed traffic

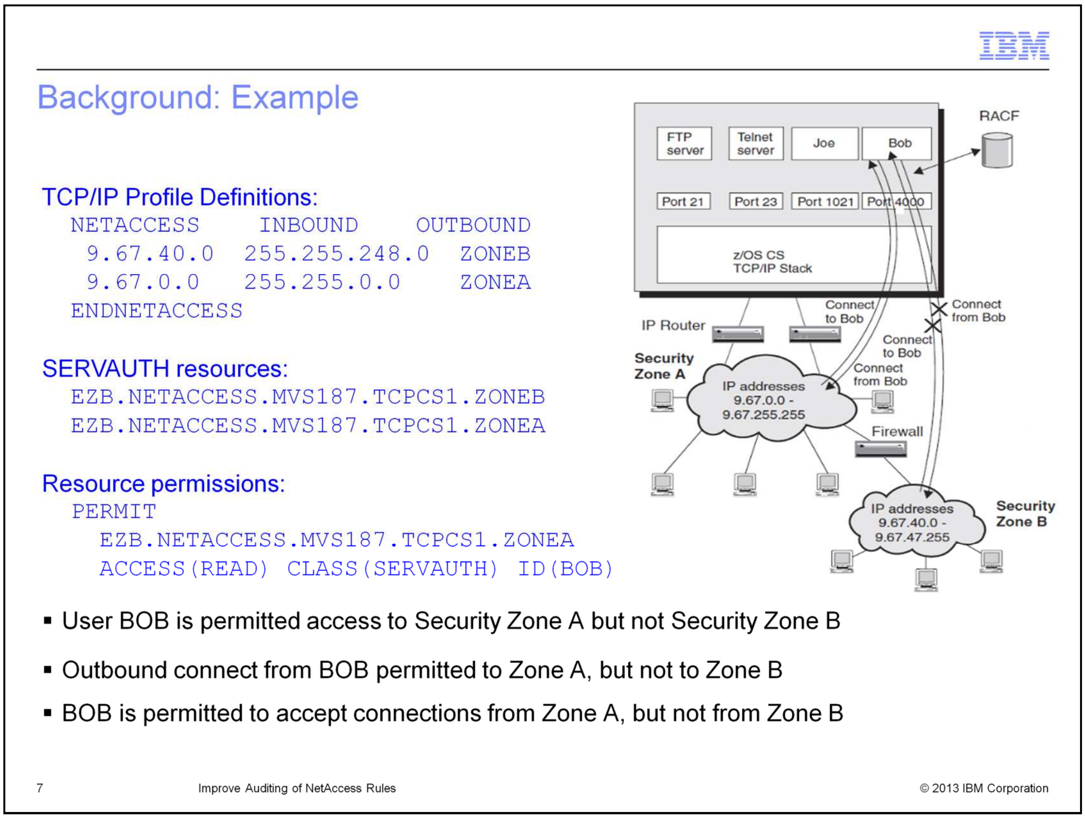
6 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

After the setup steps needed to control access to security zones are completed, the TCP/IP stack begins controlling access.

When a socket attempts to access an IP address, the TCP/IP stack determines the most specific security zone that contains the IP address. The information defined on the NETACCESS profile statement is then used to determine the name associated with the zone and to construct the Security Access Facility resource profile name for the zone. The stack then makes a call to the Security Access Facility to check if the one who is associated with the socket has read access to the resource profile. If the one who is associated with the socket has access to the resource profile, the socket is allowed to access the IP address. Otherwise, the socket is not allowed to access the IP address.

The NETACCESS statement can be used to enable network access control for only inbound traffic, for only outbound traffic, or for both inbound and outbound traffic. If it is enabled for inbound traffic, the user's access to the local IP address is checked during bind processing and the user's access to the remote IP address is checked during accept and receive processing. If it is enabled for outbound traffic, the user's access to the remote IP address is checked during connect and send processing.

The NetAccess function does not apply to traffic that is being routed by the stack, only to traffic that originates or terminates at the stack.



Background: Example

TCP/IP Profile Definitions:

```
NETACCESS     INBOUND     OUTBOUND
  9.67.40.0  255.255.248.0  ZONEB
  9.67.0.0   255.255.0.0    ZONEA
ENDNETACCESS
```

SERVAUTH resources:

```
EZB.NETACCESS.MVS187.TCPCS1.ZONEB
EZB.NETACCESS.MVS187.TCPCS1.ZONEA
```

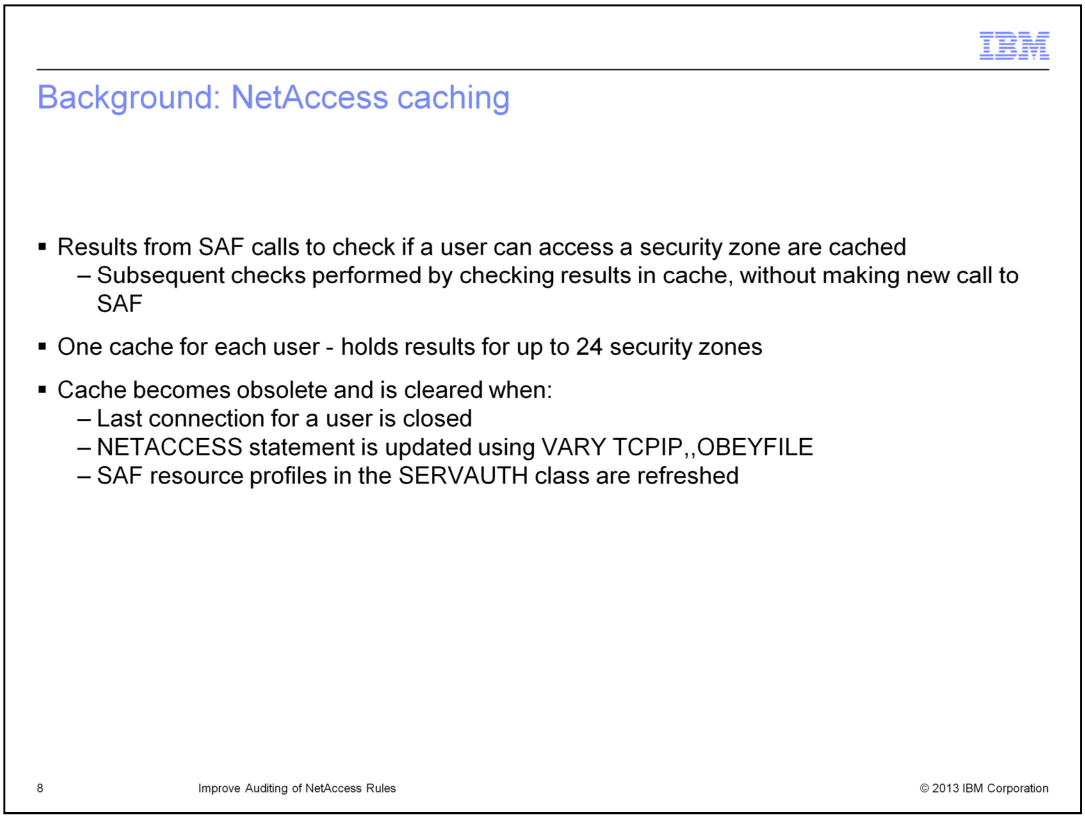
Resource permissions:

```
PERMIT
  EZB.NETACCESS.MVS187.TCPCS1.ZONEA
  ACCESS(READ) CLASS(SERVAUTH) ID(BOB)
```

- User BOB is permitted access to Security Zone A but not Security Zone B
- Outbound connect from BOB permitted to Zone A, but not to Zone B
- BOB is permitted to accept connections from Zone A, but not from Zone B

7 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

This example shows the setup steps needed to control access to two different security zones. User BOB is given access to security zone A, but not to security zone B. As a result of this setup, sockets associated with user BOB are able to access IP addresses in security zone A, but they are not able to access IP address in security zone B.



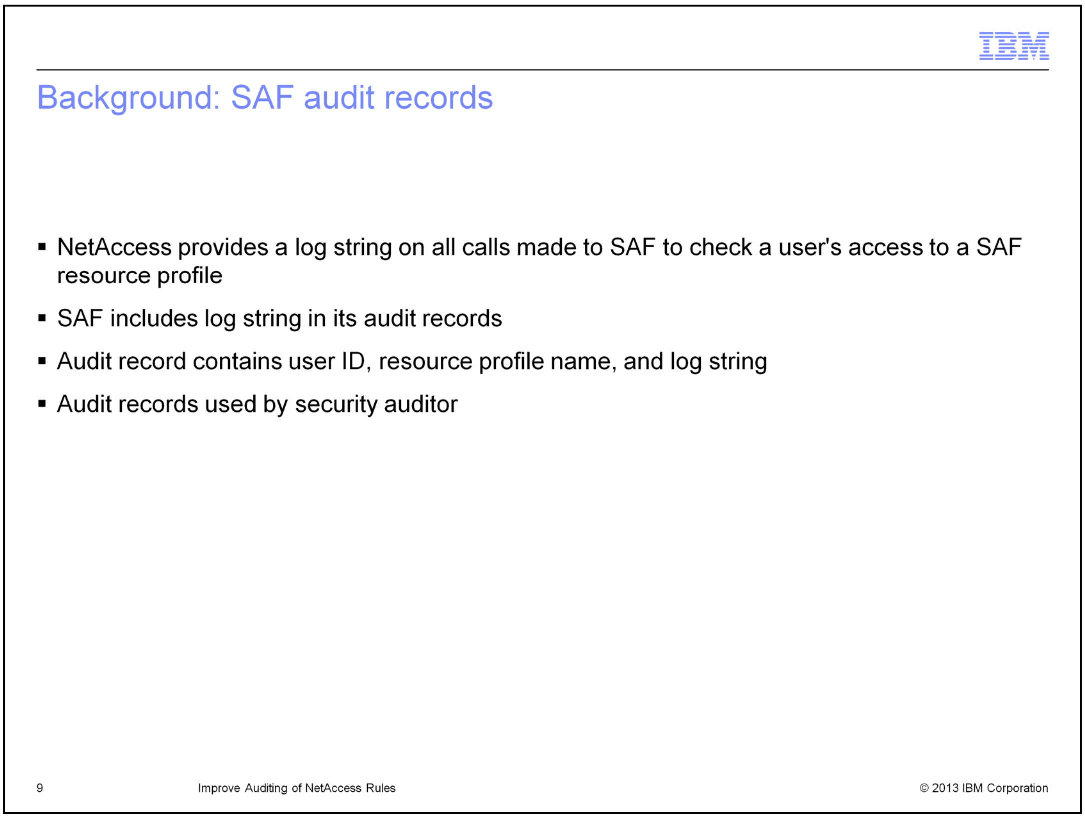
Background: NetAccess caching

- Results from SAF calls to check if a user can access a security zone are cached
  - Subsequent checks performed by checking results in cache, without making new call to SAF
- One cache for each user - holds results for up to 24 security zones
- Cache becomes obsolete and is cleared when:
  - Last connection for a user is closed
  - NETACCESS statement is updated using VARY TCPIP,,OBEYFILE
  - SAF resource profiles in the SERVAUTH class are refreshed

The implementation of the NetAccess function in z/OS Communications Server includes the caching of user access information learned from calls to the Security Access Facility. This caching is done to reduce the number of calls that are needed to the Security Access Facility. Once a user's access to a security zone has been determined, subsequent checks of that user's access to IP addresses in that security zone are completed using the information in the cache. No call to the Security Access Facility is needed.

The TCP/IP stack maintains a cache for each user whose access has been checked. The cache can hold the access information for up to twenty four different security zones.

The cache for a user is deleted when the last active connection for a user is closed. It is also deleted if the NETACCESS statement is updated using a VARY TCPIP,,OBEYFILE command or if the Security Access Facility resource profiles in the SERVAUTH class are refreshed.



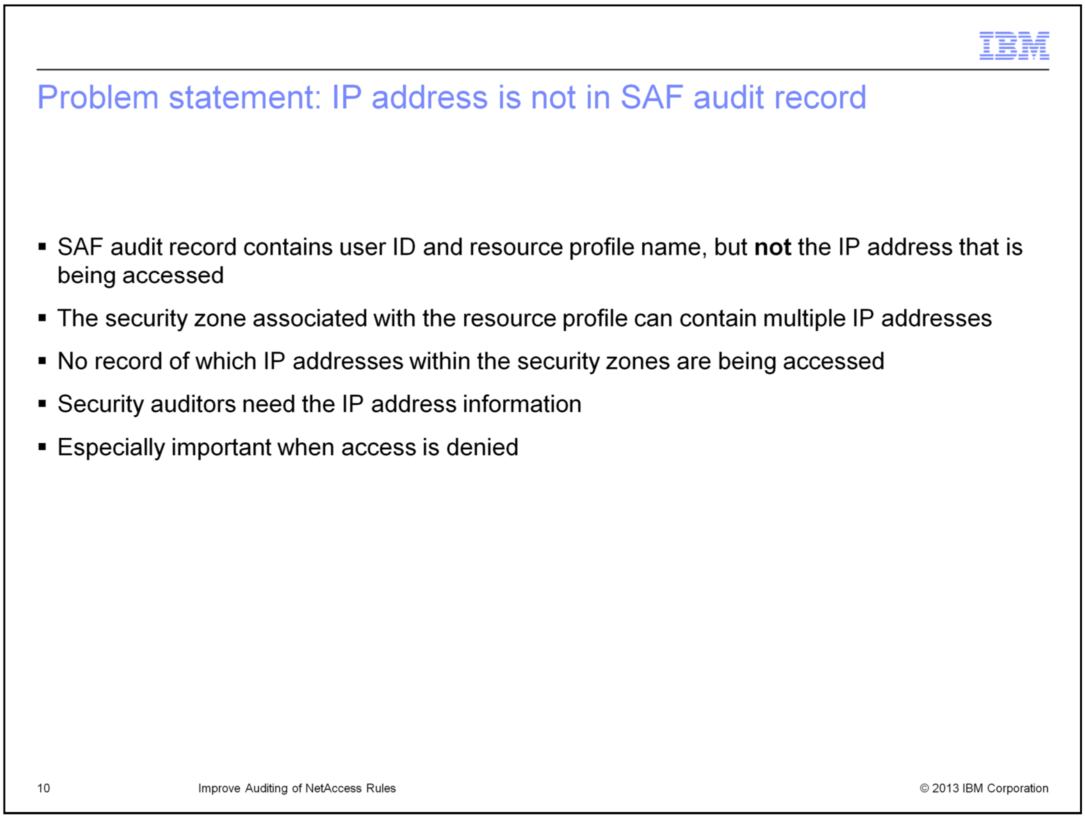
Background: SAF audit records

- NetAccess provides a log string on all calls made to SAF to check a user's access to a SAF resource profile
- SAF includes log string in its audit records
- Audit record contains user ID, resource profile name, and log string
- Audit records used by security auditor

9 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

Each time that the TCP/IP stack calls the Security Access Facility to check a user's access to a resource profile, it provides a log string. The Security Access Facility includes this log string in the audit records that it writes. If RACF is being used as the Security Access Facility, the audit record is a RACF SMF record.

The audit record contains the user ID, the name of the resource profile, and the log string provided by the stack. These Security Access Facility audit records are used by security auditors to audit network resources that users are attempting to access and network resources that are attempting to access the stack.



Problem statement: IP address is not in SAF audit record

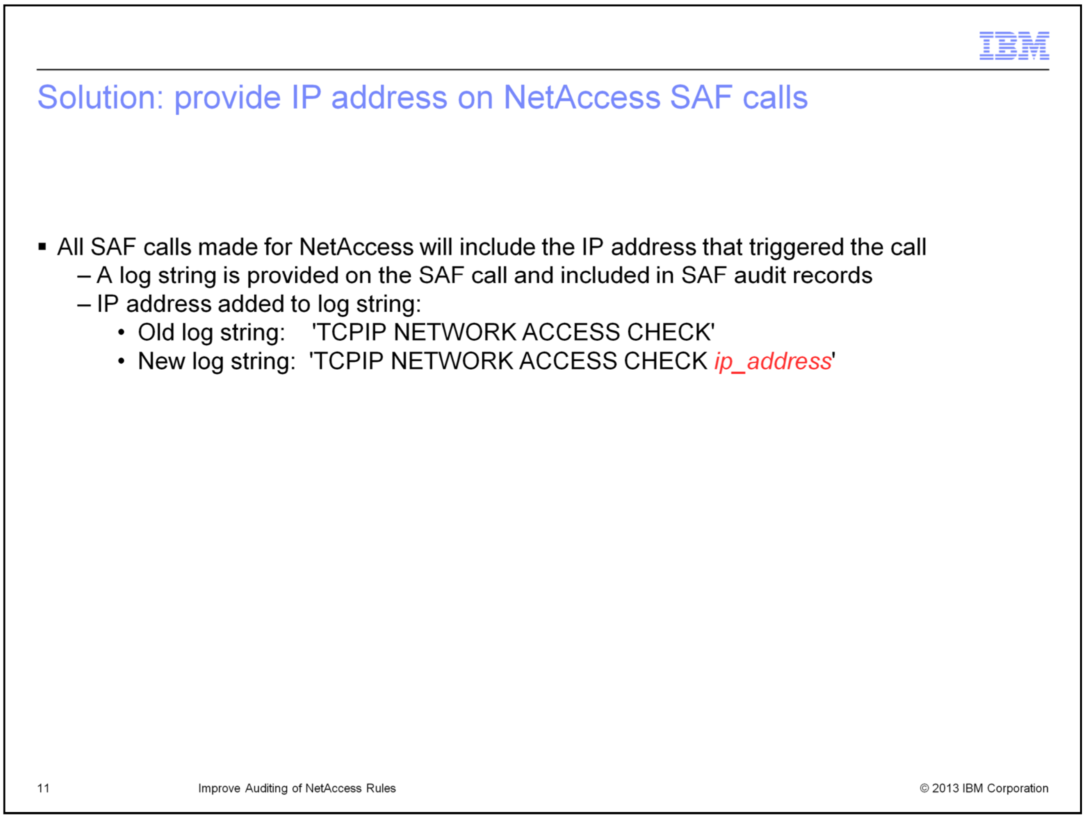
- SAF audit record contains user ID and resource profile name, but **not** the IP address that is being accessed
- The security zone associated with the resource profile can contain multiple IP addresses
- No record of which IP addresses within the security zones are being accessed
- Security auditors need the IP address information
- Especially important when access is denied

10 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

There are two problems that are being addressed by the NetAccess changes made in this release. The first problem is that the SAF audit records that are written for each call to check a user's access to a resource profile do not contain the IP address that a user is attempting to access.

The information that is included, user ID and resource profile name, allow a security auditor to determine which security zones are being accessed by users. However, a network zone can contain multiple IP addresses. Without the IP address in the records, the auditor is unable to determine the IP addresses that are being accessed.

The IP address information, which is especially important when access is not permitted to the security zone, has been requested by security auditors.

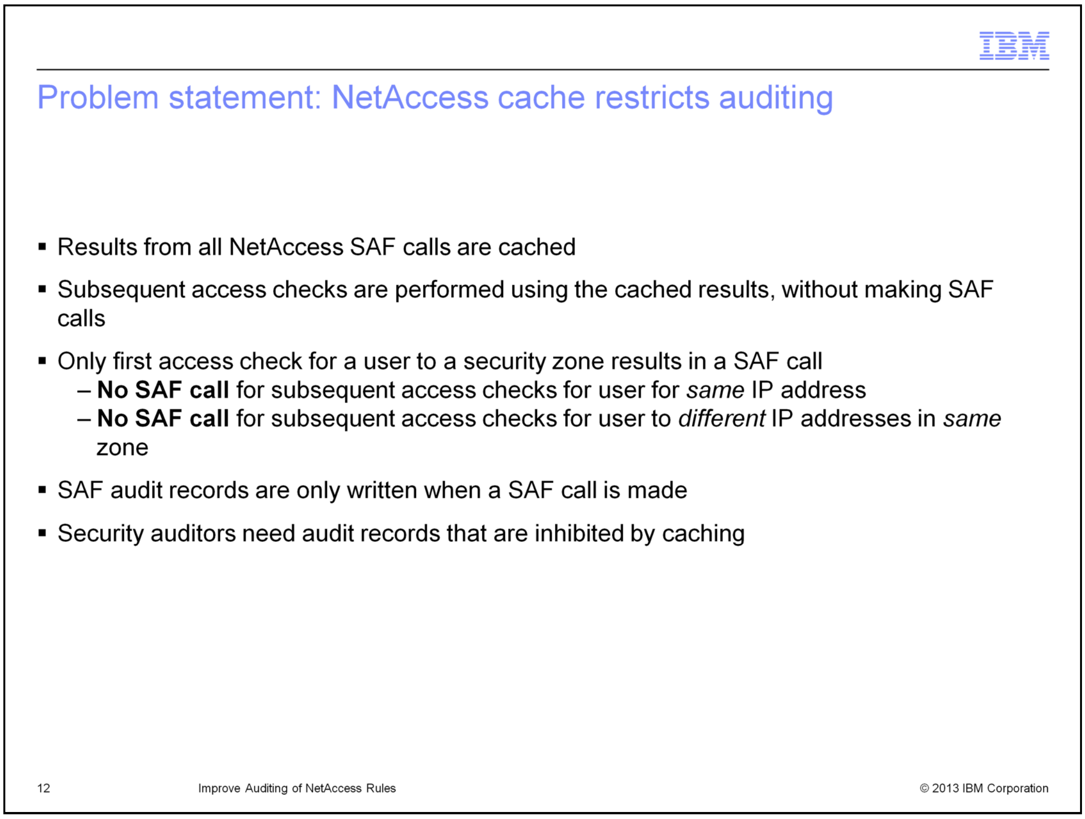


Solution: provide IP address on NetAccess SAF calls

- All SAF calls made for NetAccess will include the IP address that triggered the call
  - A log string is provided on the SAF call and included in SAF audit records
  - IP address added to log string:
    - Old log string: 'TCPIP NETWORK ACCESS CHECK'
    - New log string: 'TCPIP NETWORK ACCESS CHECK *ip_address*'

11 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

To address this first problem, all calls made to the Security Access Facility for NetAccess now include the IP address that triggered the call. The IP address is included in the log string that is provided as a parameter on the Security Access Facility call and which the Security Access Facility includes as part of the audit record that it writes.



IBM

Problem statement: NetAccess cache restricts auditing

- Results from all NetAccess SAF calls are cached
- Subsequent access checks are performed using the cached results, without making SAF calls
- Only first access check for a user to a security zone results in a SAF call
  - **No SAF call** for subsequent access checks for user for *same* IP address
  - **No SAF call** for subsequent access checks for user to *different* IP addresses in *same* zone
- SAF audit records are only written when a SAF call is made
- Security auditors need audit records that are inhibited by caching

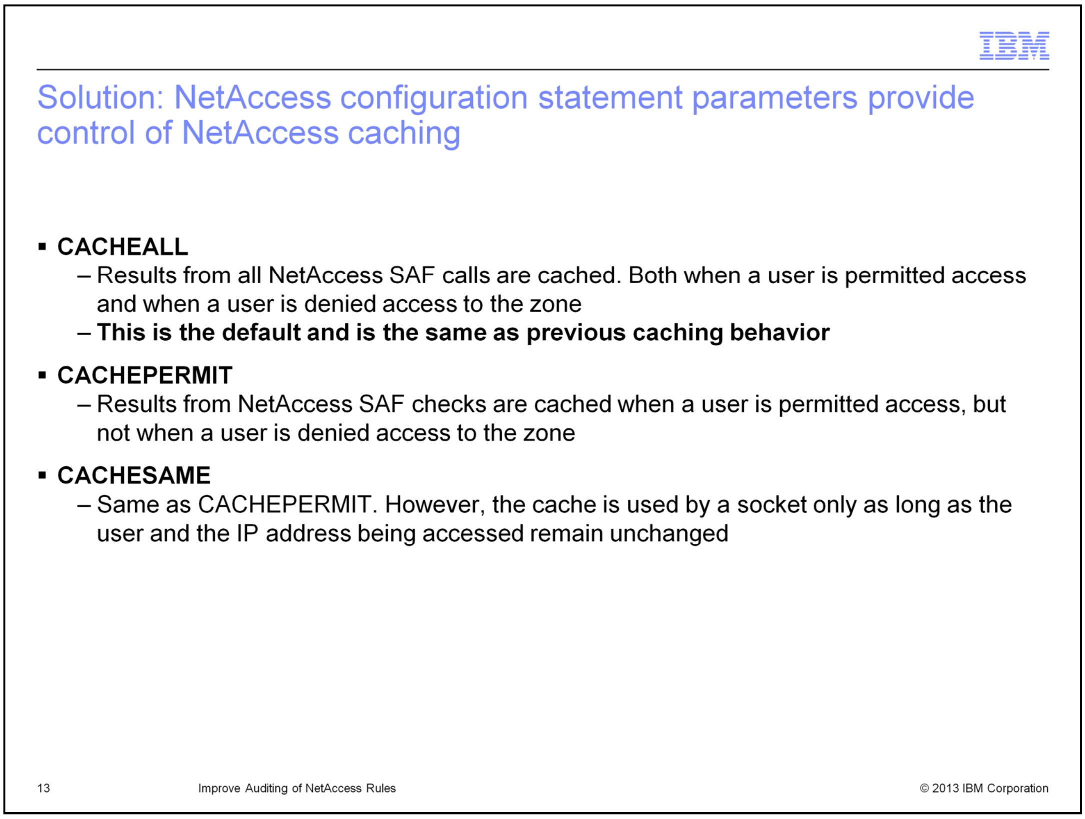
12 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

The second problem that is being addressed by the NetAccess changes made in this release is that the caching performed by NetAccess restricts the information available to security auditors.

As discussed in the background information, results from NetAccess calls to the Security Access Facility are cached and subsequent access checks are completed using the cache. When the cache is used, no call is made to the Security Access Facility. What this means is that only the first access check for a user to a particular security zone results in a call to the Security Access Facility. Subsequent checks for a user for the same IP address or for any other IP address in the same security zone do not result in a new call.

Security auditors use Security Access Facility audit records to determine the network resources that users are attempting to access and the network resources that are attempting to access the stack. These audit records can only be written by the Security Access facility when it is called.

Since NetAccess caching reduces the number of NetAccess-related audit records, it is difficult for security auditors to get a full picture of the resources being accessed and the resources accessing the stack.



Solution: NetAccess configuration statement parameters provide control of NetAccess caching

- **CACHEALL**
  - Results from all NetAccess SAF calls are cached. Both when a user is permitted access and when a user is denied access to the zone
  - **This is the default and is the same as previous caching behavior**
- **CACHEPERMIT**
  - Results from NetAccess SAF checks are cached when a user is permitted access, but not when a user is denied access to the zone
- **CACHESAME**
  - Same as CACHEPERMIT. However, the cache is used by a socket only as long as the user and the IP address being accessed remain unchanged

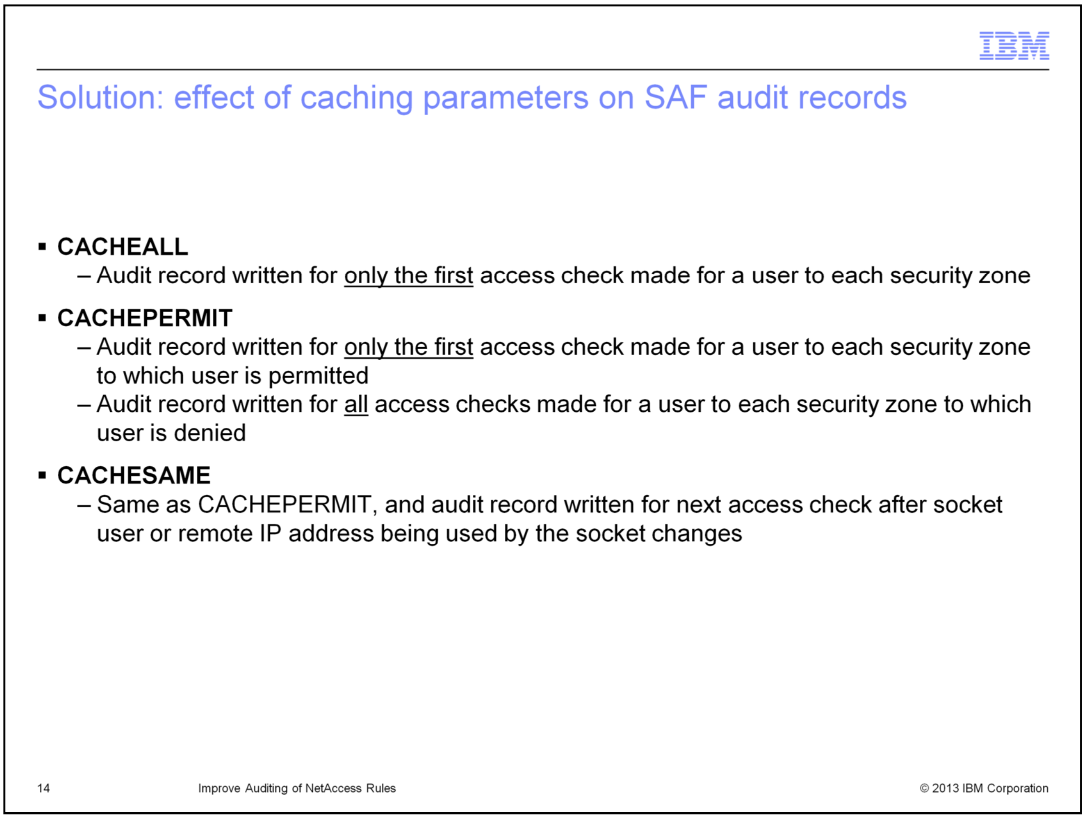
13 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

To address this problem, three parameters are added to the NETACCESS configuration statement in the TCP/IP profile. These parameters, CACHEALL, CACHEPERMIT, and CACHESAME, allow you to control the level of caching that is used by NetAccess.

When the CACHEALL parameter is specified, the results from all NetAccess calls made to the Security Access Facility are cached. This is true both when a user is permitted access to the security zone and when a user is denied access. This is the default when no caching level is specified and is same as the NetAccess caching behavior that has existed in the past.

When the CACHEPERMIT parameter is specified, the results from NetAccess calls made to the Security Access Facility are cached when a user is permitted access to the security zone. However, the results are not cached when a user is denied access to the security zone.

When the CACHESAME parameter is specified, the caching behavior is the same as with CACHEPERMIT. However, when CACHEALL and CACHEPERMIT are specified, the results in the cache are always used when they are available. Conversely, when CACHESAME is specified, the results in the cache are used by a socket only as long as the user and the IP address being accessed remain unchanged.



Solution: effect of caching parameters on SAF audit records

- **CACHEALL**
  - Audit record written for only the first access check made for a user to each security zone
- **CACHEPERMIT**
  - Audit record written for only the first access check made for a user to each security zone to which user is permitted
  - Audit record written for all access checks made for a user to each security zone to which user is denied
- **CACHESAME**
  - Same as CACHEPERMIT, and audit record written for next access check after socket user or remote IP address being used by the socket changes

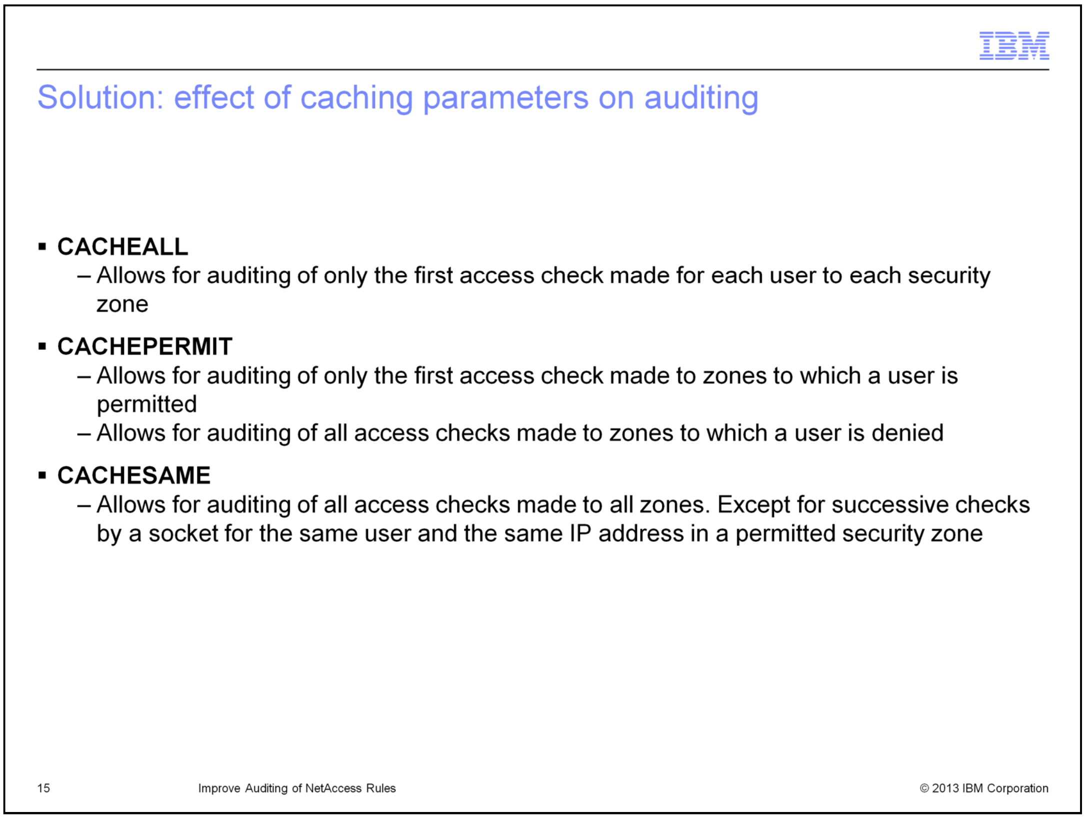
14 Improve Auditing of NetAccess Rules © 2013 IBM Corporation

So, what effect does each of the NetAccess caching levels have on the audit records written by the Security Access Facility? Remember that an audit record can only be written when a call is made to the Security Access Facility, not when the cache is used.

When the CACHEALL parameter is specified, an audit record is written for only the first access check that is made for a user to a particular security zone. This is because all other checks made for that user to either the same IP address or different IP addresses in the same security zone are completed using the results stored in the cache. This is true regardless of whether access is permitted or denied.

When the CACHEPERMIT parameter is specified, an audit record is written for only the first access check that is made for a user to a security zone to which a user is permitted. This is because, as with the CACHEALL parameter, all other checks made for that user to the same security zone are completed using the results stored in the cache. However, an audit record is written for every check in which access is denied. This is because results are not cached when a user is denied access to the security zone.

When the CACHESAME parameter is specified, audit records are written in the same instances as they are when the CACHEPERMIT parameter is specified. In addition, an audit record is written for the next access check in which the one associated with the socket changes or the remote IP address being accessed by the socket changes.



Solution: effect of caching parameters on auditing

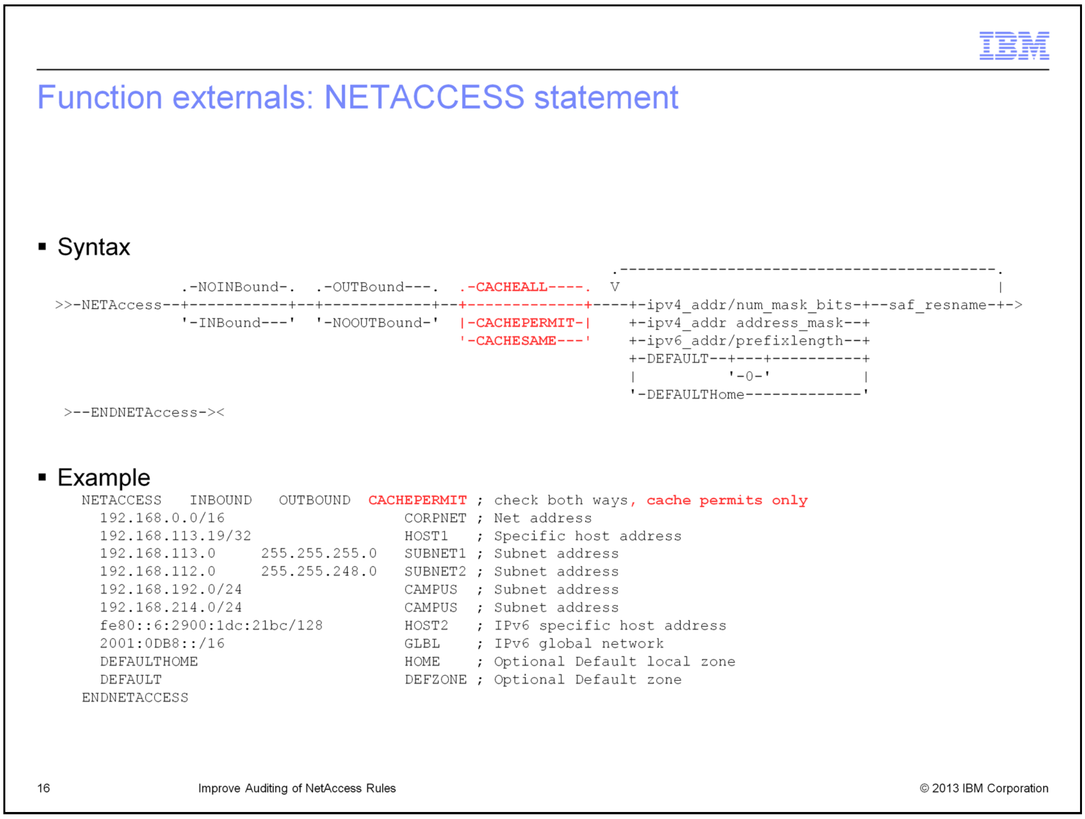
- **CACHEALL**
  - Allows for auditing of only the first access check made for each user to each security zone
- **CACHEPERMIT**
  - Allows for auditing of only the first access check made to zones to which a user is permitted
  - Allows for auditing of all access checks made to zones to which a user is denied
- **CACHESAME**
  - Allows for auditing of all access checks made to all zones. Except for successive checks by a socket for the same user and the same IP address in a permitted security zone

Finally, what effect does each of the NetAccess caching levels have on auditing?

When the CACHEALL parameter is specified, the result is the same behavior as has existed in the past. The auditor can audit only the first access check made for each user to each security zone.

When the CACHEPERMIT parameter is specified, the auditor can audit only the first access check made for each user to security zones to which a user is permitted access. However, the auditor can audit all access checks made to security zones to which a user is denied access. This is important because access attempts that are not permitted are typically of more interest to an auditor.

When the CACHESAME parameter is specified, the auditor can, with one exception, audit all access checks made to all zones. Zones include those to which a user is permitted and those to which a user is denied. The one exception is for successive checks by a socket for the same user and the same IP address in a permitted security zone. Repeated audit records for the same socket user accessing the same IP address to which it is permitted access are not of great interest to an auditor. Providing such records will greatly increase the number of audit records written and will affect performance.



Function externals: NETACCESS statement

- Syntax

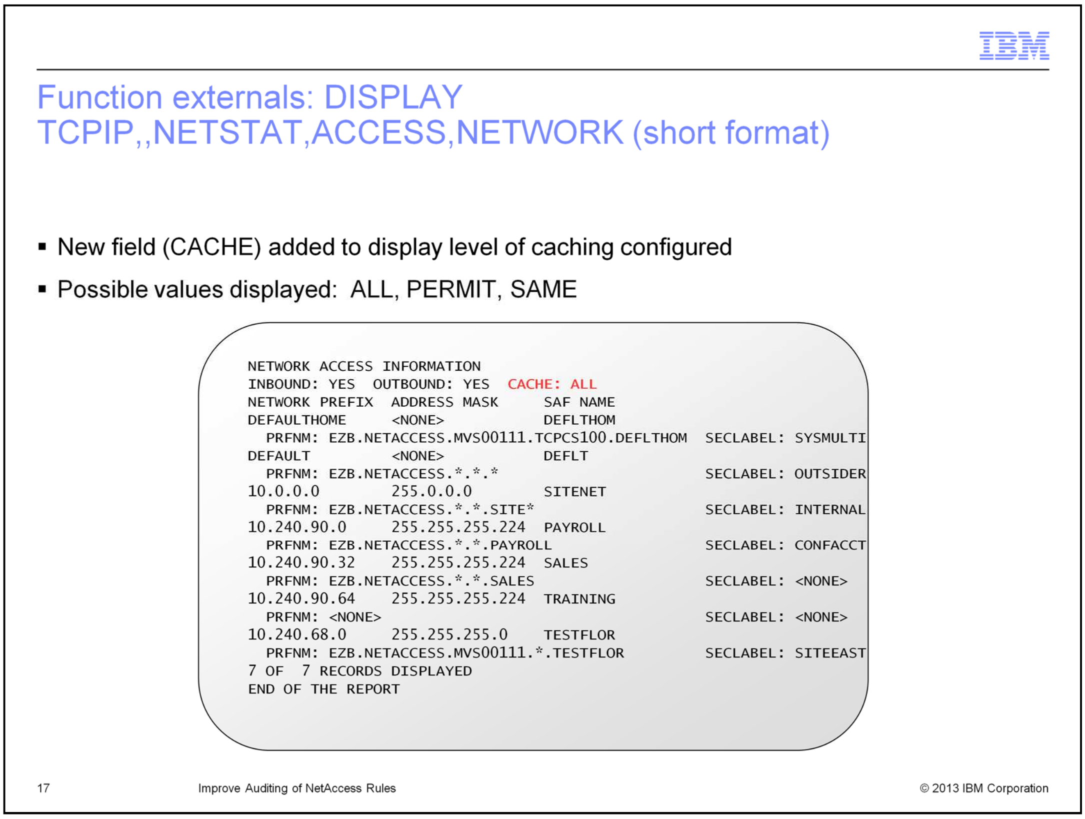
```
                                                              .------------------------------------------.
              .-NOINBound-.  .-OUTBound---.  .-CACHEALL----.  V                                          |
>>-NETAccess--+-----------+--+------------+--+-------------+----+-ipv4_addr/num_mask_bits-+--saf_resname-+->
              '-INBound---'  '-NOOUTBound-'  |-CACHEPERMIT-|    +-ipv4_addr address_mask--+
                                             '-CACHESAME---'    +-ipv6_addr/prefixlength--+
                                                                +-DEFAULT--+---+----------+
                                                                |          '-0-'          |
                                                                '-DEFAULTHome-------------'

 >--ENDNETAccess-><
```

- Example

```
NETACCESS   INBOUND   OUTBOUND  CACHEPERMIT ; check both ways, cache permits only
  192.168.0.0/16                    CORPNET ; Net address
  192.168.113.19/32                 HOST1   ; Specific host address
  192.168.113.0     255.255.255.0   SUBNET1 ; Subnet address
  192.168.112.0     255.255.248.0   SUBNET2 ; Subnet address
  192.168.192.0/24                  CAMPUS  ; Subnet address
  192.168.214.0/24                  CAMPUS  ; Subnet address
  fe80::6:2900:1dc:21bc/128         HOST2   ; IPv6 specific host address
  2001:0DB8::/16                    GLBL    ; IPv6 global network
  DEFAULTHOME                       HOME    ; Optional Default local zone
  DEFAULT                           DEFZONE ; Optional Default zone
ENDNETACCESS
```

16 Improve Auditing of NetAccess Rules

The NETACCESS statement in the TCP/IP profile is modified to add three parameters to provide control of NetAccess caching. The new parameters, CACHEALL, CACHEPERMIT, and CACHESAME, can be specified on the NETACCESS statement as shown in the syntax diagram. The example shows a configured NETACCESS statement with CACHEPERMIT specified.



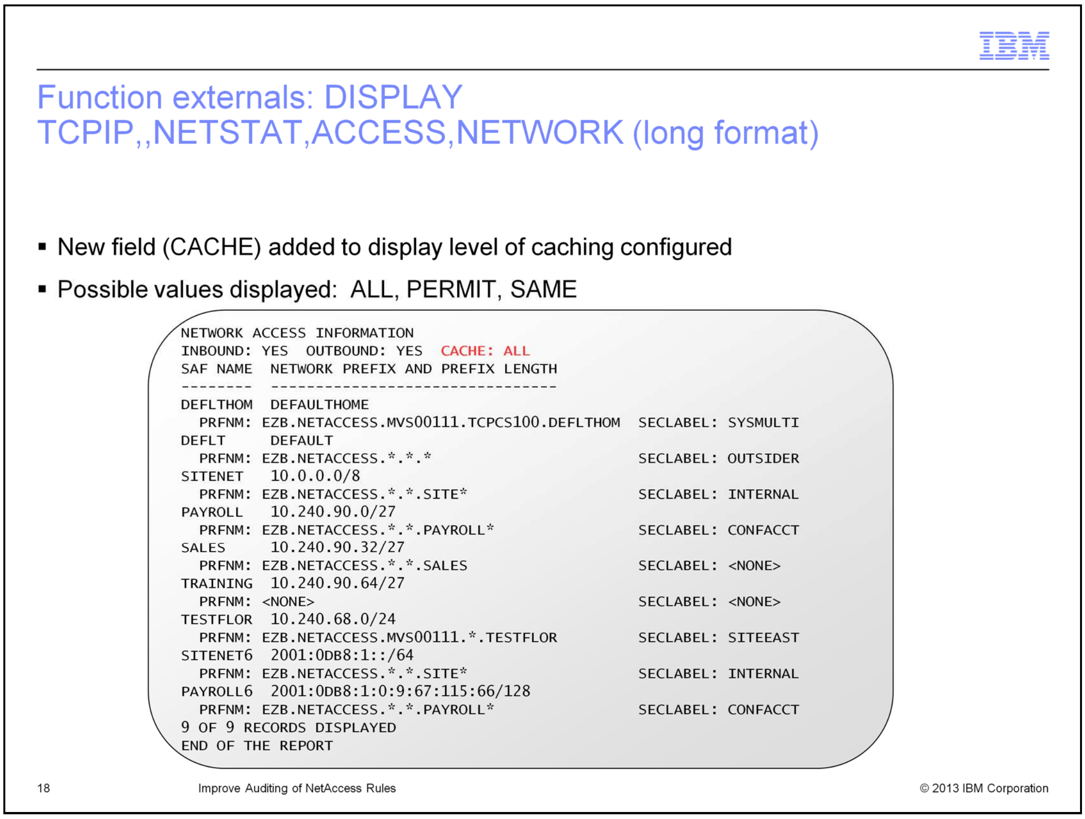
Function externals: DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK (short format)

- New field (CACHE) added to display level of caching configured
- Possible values displayed: ALL, PERMIT, SAME

```
NETWORK ACCESS INFORMATION
INBOUND: YES  OUTBOUND: YES  CACHE: ALL
NETWORK PREFIX  ADDRESS MASK     SAF NAME
DEFAULTHOME     <NONE>           DEFLTHOM
  PRFNM: EZB.NETACCESS.MVS00111.TCPCS100.DEFLTHOM  SECLABEL: SYSMULTI
DEFAULT         <NONE>           DEFLT
  PRFNM: EZB.NETACCESS.*.*.*                       SECLABEL: OUTSIDER
10.0.0.0        255.0.0.0        SITENET
  PRFNM: EZB.NETACCESS.*.*.SITE*                   SECLABEL: INTERNAL
10.240.90.0     255.255.255.224  PAYROLL
  PRFNM: EZB.NETACCESS.*.*.PAYROLL                 SECLABEL: CONFACCT
10.240.90.32    255.255.255.224  SALES
  PRFNM: EZB.NETACCESS.*.*.SALES                   SECLABEL: <NONE>
10.240.90.64    255.255.255.224  TRAINING
  PRFNM: <NONE>                                    SECLABEL: <NONE>
10.240.68.0     255.255.255.0    TESTFLOR
  PRFNM: EZB.NETACCESS.MVS00111.*.TESTFLOR         SECLABEL: SITEEAST
7 OF  7 RECORDS DISPLAYED
END OF THE REPORT
```

The report that is displayed in response to a DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK command is modified to include the level of caching that is configured for NetAccess. The possible values in the new CACHE field are ALL, PERMIT, and SAME.

The example shows the new CACHE field in the short format of the report.



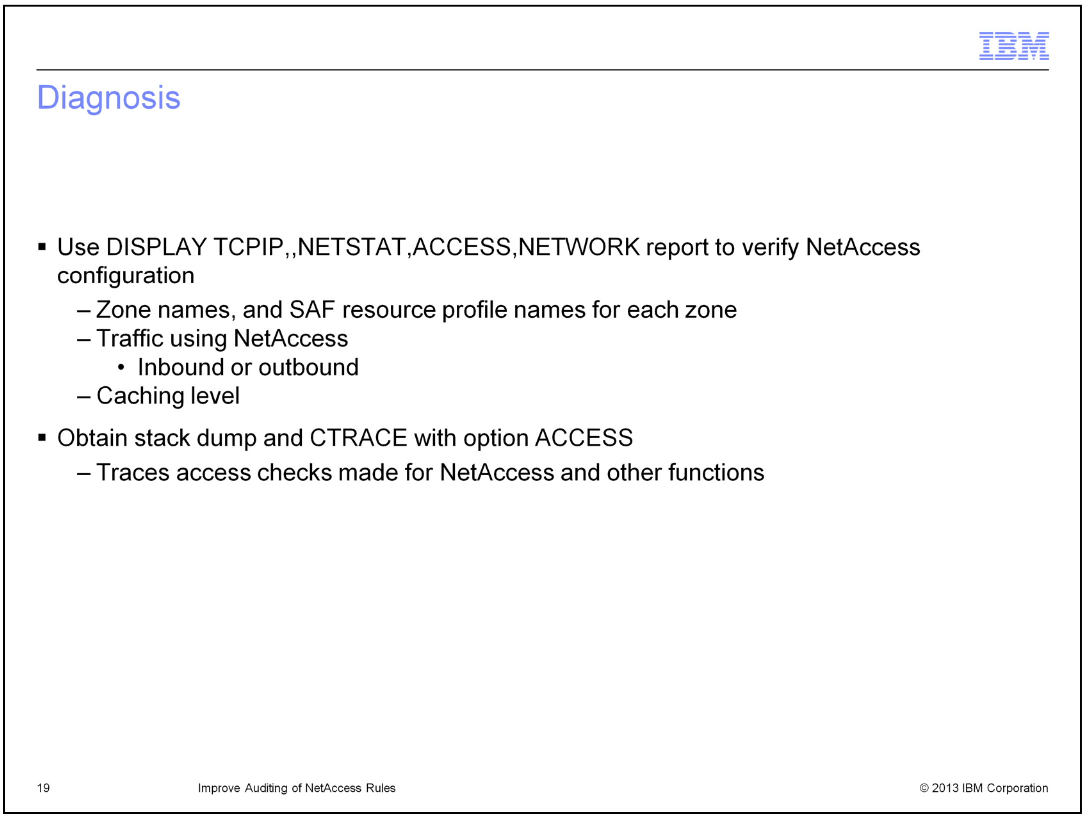
Function externals: DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK (long format)

- New field (CACHE) added to display level of caching configured
- Possible values displayed: ALL, PERMIT, SAME

```
NETWORK ACCESS INFORMATION
INBOUND: YES  OUTBOUND: YES  CACHE: ALL
SAF NAME  NETWORK PREFIX AND PREFIX LENGTH
--------  --------------------------------
DEFLTHOM  DEFAULTHOME
  PRFNM: EZB.NETACCESS.MVS00111.TCPCS100.DEFLTHOM  SECLABEL: SYSMULTI
DEFLT     DEFAULT
  PRFNM: EZB.NETACCESS.*.*.*                       SECLABEL: OUTSIDER
SITENET   10.0.0.0/8
  PRFNM: EZB.NETACCESS.*.*.SITE*                   SECLABEL: INTERNAL
PAYROLL   10.240.90.0/27
  PRFNM: EZB.NETACCESS.*.*.PAYROLL*                SECLABEL: CONFACCT
SALES     10.240.90.32/27
  PRFNM: EZB.NETACCESS.*.*.SALES                   SECLABEL: <NONE>
TRAINING  10.240.90.64/27
  PRFNM: <NONE>                                    SECLABEL: <NONE>
TESTFLOR  10.240.68.0/24
  PRFNM: EZB.NETACCESS.MVS00111.*.TESTFLOR         SECLABEL: SITEEAST
SITENET6  2001:0DB8:1::/64
  PRFNM: EZB.NETACCESS.*.*.SITE*                   SECLABEL: INTERNAL
PAYROLL6  2001:0DB8:1:0:9:67:115:66/128
  PRFNM: EZB.NETACCESS.*.*.PAYROLL*                SECLABEL: CONFACCT
9 OF 9 RECORDS DISPLAYED
END OF THE REPORT
```

There is also a long format of the report that is displayed in response to a DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK command. This format of the report allows for the display of longer IPv6 addresses.

This example shows the new CACHE field in the long format of the report.

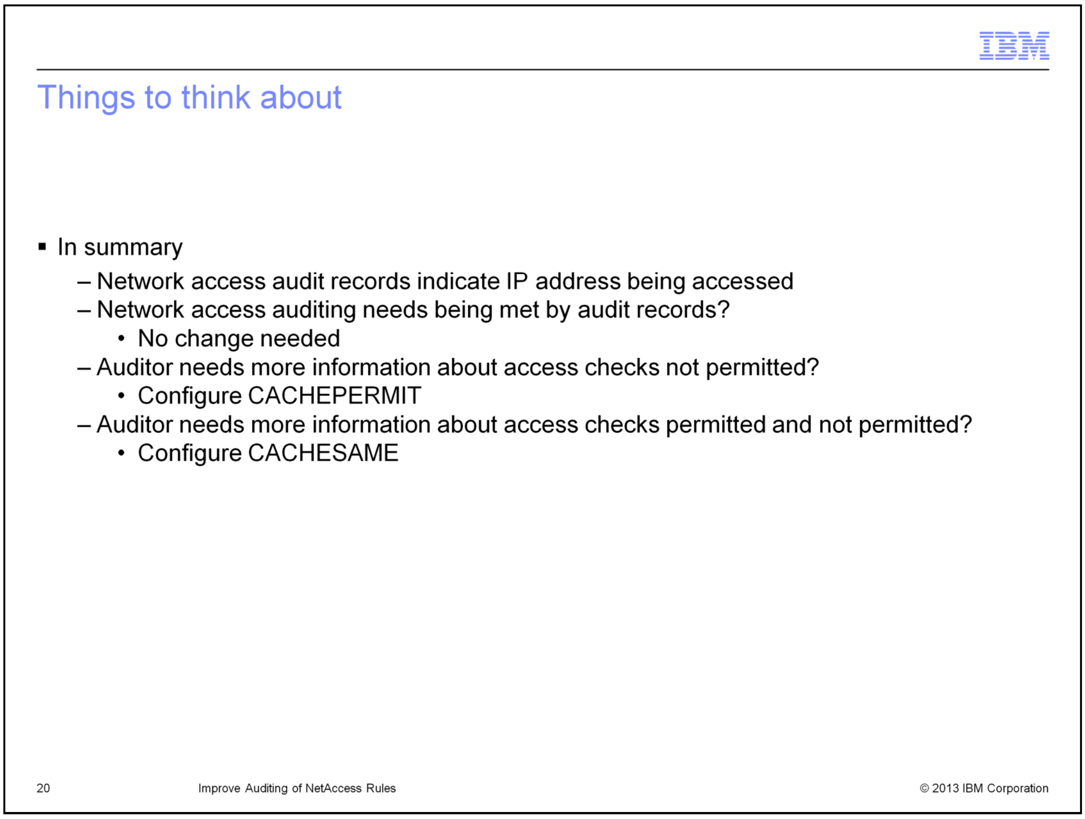


Diagnosis

- Use DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK report to verify NetAccess configuration
  - Zone names, and SAF resource profile names for each zone
  - Traffic using NetAccess
    - Inbound or outbound
  - Caching level
- Obtain stack dump and CTRACE with option ACCESS
  - Traces access checks made for NetAccess and other functions

If you experience unexpected NetAccess caching results, the first thing you should do is use the DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK command to verify your NetAccess configuration. The report displays each security zone, along with its zone name and the corresponding Security Access Facility resource profile name. Also displayed is whether inbound traffic, outbound traffic, or both are subject to NetAccess processing. Finally, the report indicates the NetAccess caching level in effect.

If you do not find any problems in your NetAccess configuration, obtain a dump of the TCP/IP stack and a CTRACE with option ACCESS. The ACCESS option traces all access checks that are made, for NetAccess and other functions.



Things to think about

- In summary
  - Network access audit records indicate IP address being accessed
  - Network access auditing needs being met by audit records?
    - No change needed
  - Auditor needs more information about access checks not permitted?
    - Configure CACHEPERMIT
  - Auditor needs more information about access checks permitted and not permitted?
    - Configure CACHESAME

To summarize, there are two enhancements made to the NetAccess function in this release. Both enhancements improve the auditing of network access checks.

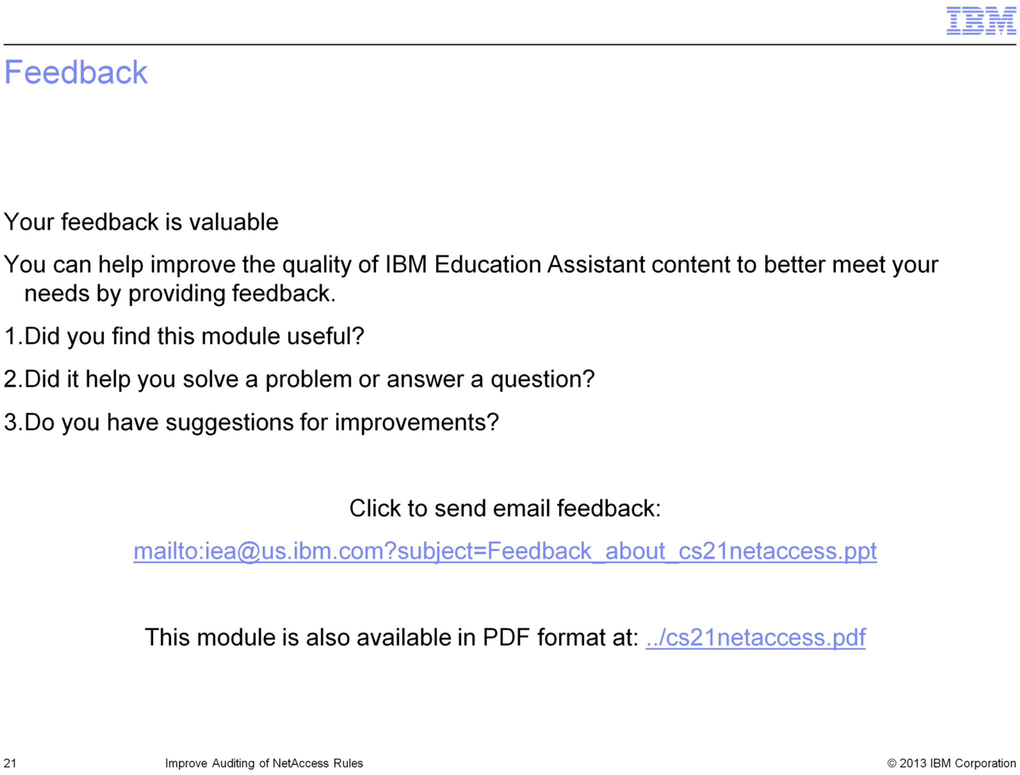
The first change improves the network access audit records by adding the IP address that triggered the check.

The second change provides control over the caching level used by NetAccess, and therefore over the audit records available to security auditors.

If your security auditor's needs relative to network access checks are being met by your existing audit records, you do not need to make any change to your configuration. You can configure the CACHEALL parameter which is the default.

If your security auditor needs more information about network access checks where a user is not permitted access to the security zone, you can configure the CACHEPERMIT parameter.

If your security auditor needs more information about network access checks both where a user is permitted and where a user is not permitted access to the security zone, you can configure the CACHESAME parameter.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

1. Did you find this module useful?
2. Did it help you solve a problem or answer a question?
3. Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_cs21netaccess.ppt

This module is also available in PDF format at: ../cs21netaccess.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.