Business Unit or Product Name

SNA Security Considerations

Thomas Cosenza

z/Center of Excellence – IBM

tcosenza@us.ibm.com

© 2007 IBM Corporation

Agenda

- **Why Add Security**
- **Overview**
- **“The Weakest Link”**
- **Security SNA Topology**
- **Searching Security**
- **Application Security**
- **Conclusion**

© 2007 IBM Corporation

Why Add Security

- ID theft is on the rise
- Meet new standards
  - PCI standard (Session S1713)
  - European Common Standard
  - US regulations starting to come around
    - California SB 1386
- Keep the business off the BLOGs
  - Was the Front Page… but these days bad news travels a lot faster

© 2007 IBM Corporation

Why Add Security

- Failure to Secure your business
  - Fines and penalties
  - Incidents from loss of data
    - Costs for forensics examinations
    - Liability for the losses
    - Dispute resolution costs
  - Stock Shares plummet
  - Loss of Customers

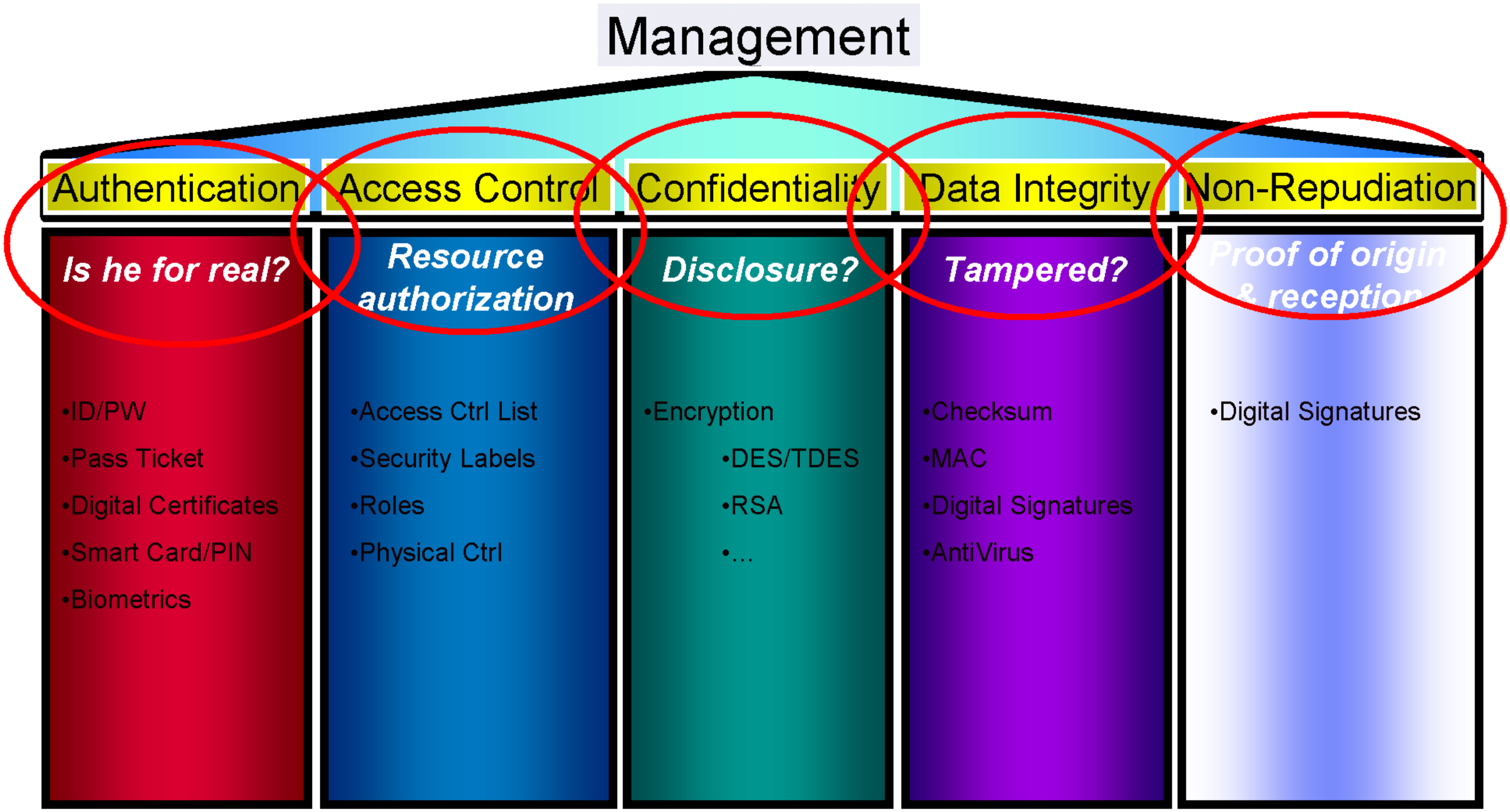
© 2007 IBM Corporation

Words to Live By

- **“The Security Perimeter is now at the End Point”**
  Anonymous

© 2007 IBM Corporation

Security Concepts



Management

Authentication

Is he for real?

- ID/PW
- Pass Ticket
- Digital Certificates
- Smart Card/PIN
- Biometrics

Access Control

Resource authorization

- Access Ctrl List
- Security Labels
- Roles
- Physical Ctrl

Confidentiality

Disclosure?

- Encryption
  - DES/TDES
  - RSA
  - …

Data Integrity

Tampered?

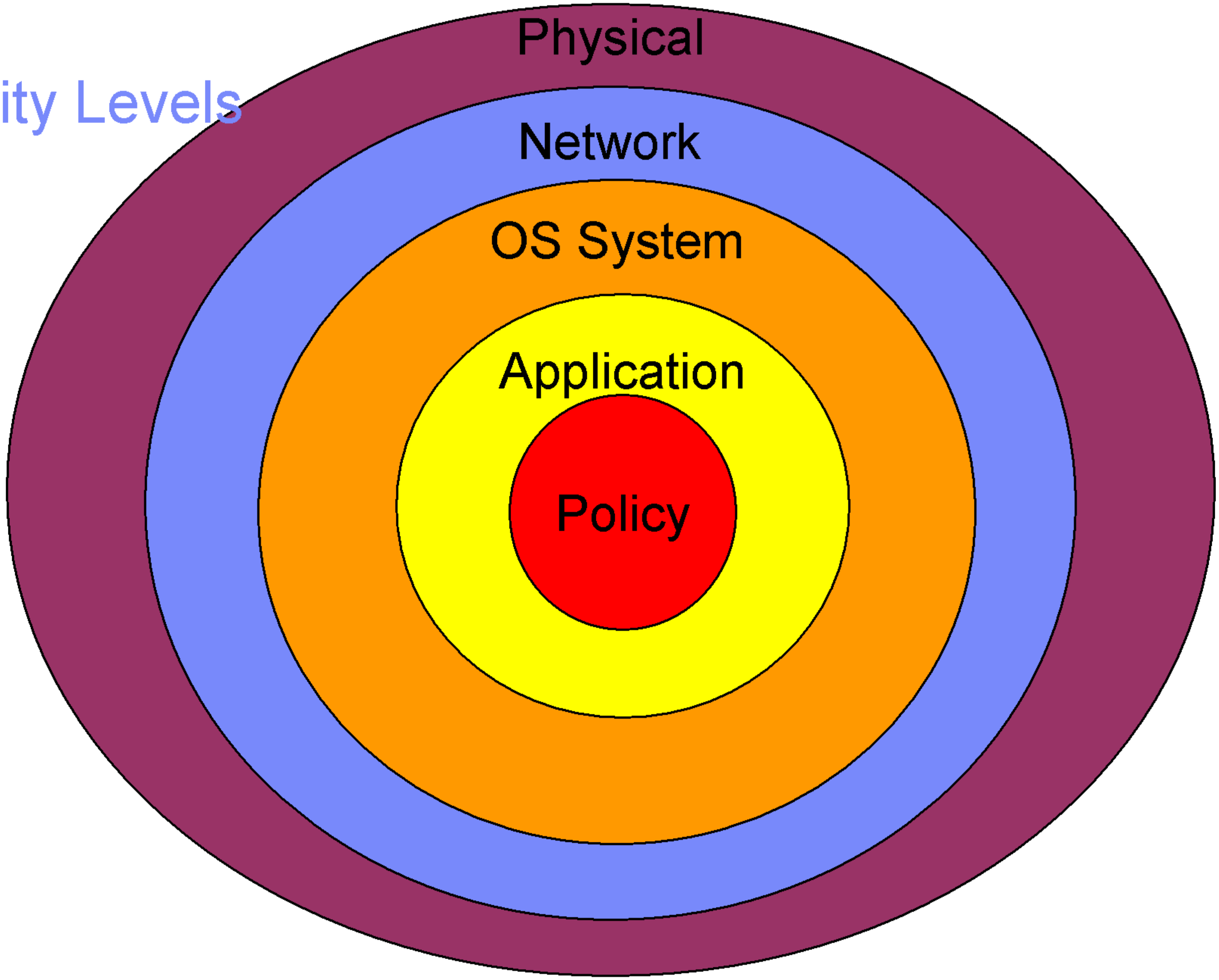
- Checksum
- MAC
- Digital Signatures
- AntiVirus

Non-Repudiation

Proof of origin & reception

- Digital Signatures

Security Levels



© 2007 IBM Corporation

State Of SNA Security

- **In the Past**
  - SNA enjoyed strong Physical Security
    - Limited Dynamic Definitions
    - Pre-Defined LUs
    - Most Wires were Contained within Walls of buildings
  - SUBAREA had strict Hierarchal Structure
  - Most terminals had no way to interface into the SNA network directly
- **What has happened**
  - Need for a more Dynamic Environment for Scalability
  - Shift Of Focus
    - Moving toward eCommerce
  - Decreasing Skill sets in the industry
  - Links are now running over IP
    - TN3270
    - Enterprise Extender,
    - DLSw

© 2007 IBM Corporation

Types of attackers

- **Well the Good news**
  - A majority of general network attacks are done by novice hackers
    - Kiddie Scripter
    - People more interested in bringing down systems
  - Harder to Hack SNA networks
    - PEER to PEER nature of SNA
    - Lack of available entry points compared to IP
      - (I go to my local bagel shop to get on to an IP network)
    - The multi-tier connectivity flow
- **The Bad News**
  - Organized crime and unorthodox governments have the resources to hire Career Criminals
  - Even today SNA transactions carry a large amount of confidential data
- **While IP attacks may have a greater rate of occurrence; attacks on an SNA network can provide a bigger payday**

© 2007 IBM Corporation

The Goal

- When dealing in security you have to balance what your needs of security with what the cost of that security is
- This presentation should help you identify areas in your SNA security that you can improve upon

So Basically Dont be this Guy!!!

_INFRASTRUCT

_DAY 68: Mar
didn't we id
there? We n

_Gil installe
everything.

_DAY 70: I'm
IBM experts
for quality
control and
and manage
authenticat
help make u

_The cameras

© 2007 IBM Corporation

Policy Security

- **Policy Security Is the Backbone of any good security**
  - An Organizational statement of how Data and Communications are to be governed
  - This is Independent of any Technology
  - Needs have signoff from C level types

© 2007 IBM Corporation

Policy Security

- **Separating Different Environments**
  - Do you have this
    - Your Production Environment
    - Your Development Environment
      - (Quasi Production Environment)
    - Your Test Environment
  - These environments usually have different levels of security however they are often connected through a SNA network using the same NETID.
  - This could allow a black hat to use a test machine to gain access to a SNA application on another system. Or worse …..
    - the black hat could know when an APPL will be down and bring up their own application where they can harvest IDs and other information.

© 2007 IBM Corporation

Policy Security

- **Separation of Duties**
  - Do not make IT Supermen!!!
  - Simple math … more people involved more likely to get caught
  - One easy way to do this in SNA is to separate the system programmers and the system operators.

© 2007 IBM Corporation

Policy Security

- **Need to Know**
  - Don’t give an employee or consultant more data then they need to their job
- **Proper Cleanup of Resources**
  - There are a lot of connections that are moving to pure IP links
  - More often then not I see the old definitions being activated automatically
  - This is a point of entry into your network that you must close

© 2007 IBM Corporation

Dealing with the "Weakest LINK" in a SNA Network

IP LINKS!!!

© 2007 IBM Corporation

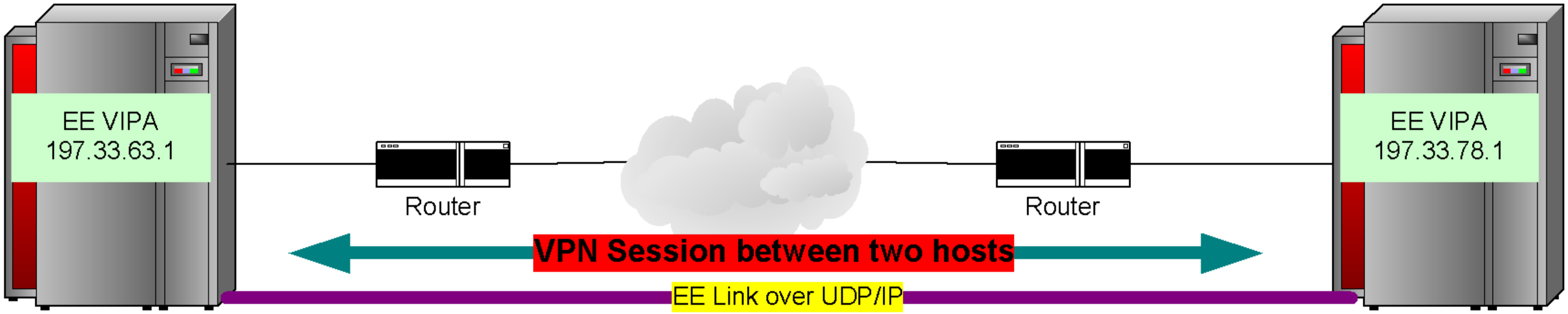
Securing IP Connections

- **SNA is a PEER to PEER environment so protecting the connections in and out of the SNA network is critical.**
- **In the Past SNA had strong Physical Security**
  - Leased Lines
  - Coded LU names
  - Hardwired to a 3745
- **SNA networks using IP links is the dominant type of connection today**
  - Enterprise Extender
  - TN3270
  - DLSW+
- **SNA environments are utilizing more IP links everyday**
  - IP links which are much more vulnerable to attack
- **So we want to protect our “weakest” links in our SNA network**

© 2007 IBM Corporation

Securing Enterprise Extender

- **Enterprise Extender has “Two Hats”**
  - SNA Hat
    - EE looks like a NIC to VTAM
  - IP Hat
    - VTAM looks like a UDP application
- **IPSec can be used to protect EE transmission**
  - IPSec has two types of Security Protocols
    - AH or ESP with Authentications
    - Can protect End to End or can protect only parts of a path



© 2007 IBM Corporation

What about other types of connections

- **TN3270 Connections**
  - TN3270 is the main way that most users access SNA applications
  - There are several SSL options that can be used to protect the data flow
    - SSL Types
      - Server Side SSL (Confidentiality and Authentication of Server)
      - Client Side SSL (Confidentiality and Authentication of both)
    - Complete Control of Encryption used
    - Can use ICSF to secure private keys
    - Can restrict access to particular applications from particular IP sites
    - Can run separate TN3270 Ports for sensitive and non-sensitive applications on the same LPAR

© 2007 IBM Corporation

What about other types of connections

- **DLSW connections**
  - Used for connecting SNA environments
  - Can be secured via
    - Encrypted Link
    - IPSec
    - Firewall Filters (not encrypted)
  - Be careful about running DLSW routers in passive mode

© 2007 IBM Corporation

Protecting Network Resources

© 2007 IBM Corporation

Securing CPCP sessions

- **CPCP sessions allow for resources to be found and sessions to be started**
- **There is a recommended guideline for dealing with SNA LU connections**
  - “Allow native SNA connections to be dynamically defined, but predefine any non-native SNA connections.”
- **The easiest way to do this for CPCP sessions is as follows.**
  - On the DYNADJCP Start option code NO
  - On any local switch major node that is for native connections override the start option to be yes
  - For non-native connections code an entry in an Adjacent CP Major Node
- **This will secure your systems from allowing any non-predefined nodes connect to your system**

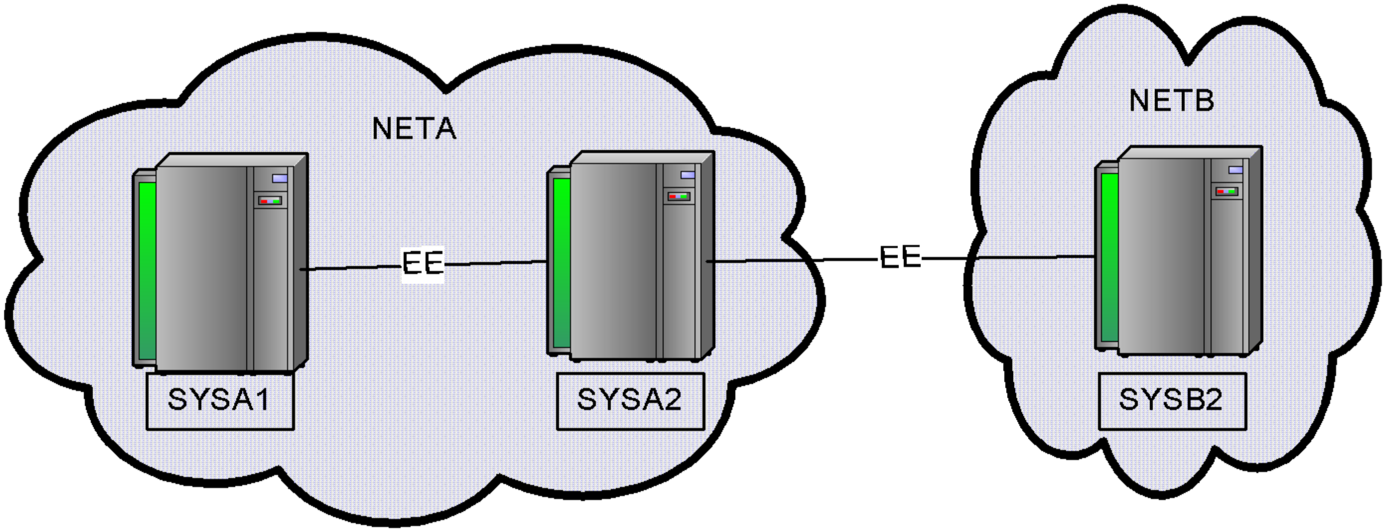
© 2007 IBM Corporation

Authenticating Nodes

- **So we go through the act of allowing CPCP sessions however how do we verify the other side**
  - APPN connections
    - Verify CP Start option
      - Uses a static Triple DES Key
      - Requires a Racf Definition
    - IPSec with EE connection
      - Can use an end to end AH or ESP with Authentication Tunnel
        - Uses Rotating Keys
        - Uses MD5 or SHA one way hash
- **Also both APPN and SUBAREA can use Session Level Encryption**
  - Uses static TripleDES keys
  - Manual Key Management
  - Good for Encrypting End to End LULU sessions

© 2007 IBM Corporation

Example Case Study



© 2007 IBM Corporation

Putting it all together

ATCSTRXX member

```
....
DYNADJCP=NO,                                              X
.......
```

EESMN

```
SHARE    VBUILD TYPE=SWNET
*
***********
*
EENAT  PU    TGP=COS1,TGN=1,PUTYPE=2,CAPACITY=100M   X
             CPCP=YES, CPNAME=SYSA1,NETID=NETA,      X
              DYNADJCP=YES
PATH1  PATH  GRPNM=&SYSNAME(1:2).GPEE,               X
                IPADDR=9.9.9.9,SAPADDR=4
*
EENON  PU    TGP=COS1,TGN=1,PUTYPE=2,CAPACITY=100M   X
             CPCP=YES, CPNAME=SYSB2,NETID=NETB
PATH2  PATH  GRPNM=&SYSNAME(1:2).GPEE,
     IPADDR=5.5.5.5, SAPADDR=4                       X
```

ADJC CP Definitions

```
NETBCP    VBUILD TYPE=ADJCP
SYSB2     ADJCP NETID=NETB,NATIVE=NO,NN=YES
```

This is on SYSA2

Securing Searches

- **SNA networks are no longer only contained within an organizations**
- **The ability to connect to Applications in other networks is the key to moving your business along**
  - Dealing with Credit Transactions
  - Checking for Inventory
  - Dealing with Healthcare information
- **The first thing that you have to know is where a search request comes from**
  - SUBAREA?
  - APPN?

© 2007 IBM Corporation

Subarea Searches

- **If the search comes from a subarea environment there are 4 options that will play a factor**
  - SORDER & SSCPORD
    - Effects the order in which a search will occur
  - SSCPDYN & DYNASSCP
    - Effects what will be searched
- **You can use a Services Management Exit to control searches as well**

© 2007 IBM Corporation

SORDER and SSCPORD

	SORDER			
SSCPORD	APPNFRST	APPN	ADJSSCP	SUBAREA
PRIORITY	1. APPN Network 2. Learned Owner 3. Coded Owner 4. Prev. Successes 5. ADJSSCP Table 6. Prev. Failures	1. Learned Owner 2. Coded Owner 3. APPN DS DB 4. Prev. Successes 5. APPN Network 6. ADJSSCP Table 7. Prev. Failures	1. Learned Owner 2. Coded Owner 3. APPN DS DB 4. Prev. Successes 5. ADJSSCP Table 6. Prev. Failures	1. Learned Owner 2. Coded Owner 3. APPN DS DB 4. Prev. Successes 5. ADJSSCP Table 6. Prev. Failures 7. APPN Network
DEFINED	1. APPN Network 2. Learned Owner 3. Coded Owner 4. ADJSSCP Table	1. Learned Owner 2. Coded Owner 3. APPN Network 4. ADJSSCP Table	1. Learned Owner 2. Coded Owner 3. APPN DS DB 4. ADJSSCP Table	1. Learned Owner 2. Coded Owner 3. APPN DS DB 4. ADJSSCP Table 5. APPN Network

Prefers APPN ←→ Prefers Subarea

From a security standpoint the SORDER option does not have much of an impact and the SSCPORD has a minor impact

© 2007 IBM Corporation

SSCPDYN and DYNASSCP

- **VTAM can not perform a search of a subarea environment without a defined CDRM**
- **These two start options allow for dynamic updates to the adjacent SSCP tables**
  - SSCPDYN
    - Allows VTAM to add a known partner CDRM to any adjacent SSCP table if that partner sends in a session request.
  - DYNASSCP
    - Allows VTAM to create adjacent SSCP tables dynamically.
- **It is best that these options be set to NO and all subarea CDRMs are predefined using an Adjacent SSCP list**

© 2007 IBM Corporation

Services Management Exit (SME)

- **Called by Session Services**
  - This exit will only be driven during the following actions
    - Vtam initialization completes
    - Vtam termination
    - Session Establishment (Init, CDInit, InitOtherCD,BIND and RouteSetup RUs)
    - SSCP takeover
  - SME can be used for the following functions
    - Session Establishment prior to any cross domain flows
    - Session Establishment after the DLU has been determined
    - Session Authorization
    - Gateway Path selection
    - ADJSSCP selection
    - Alias Translation
    - Choosing the ER/VR that will be used to carry the RTP

© 2007 IBM Corporation

APPN searching

- **APPN will be searched if**
  - The search originates from an APPN node
  - The subarea search passes the query to APPN
- **The only way to control native APPN searches is by using a DSME exit.**
- **However there are more options for controlling non-native searches**

© 2007 IBM Corporation

Searching out

- **Boarder Nodes are a specialized network node used to connect to other NETIDs**
- **You must properly configure this node to guide a search to the right netid**
- **The following can be used to modify the searching behavior**
  - Tuning Options
    - BNDYN
    - BNORD
    - SNVC
  - Adjacent Cluster Table (ADJCLUST)
  - Directory Services Management Exit

© 2007 IBM Corporation

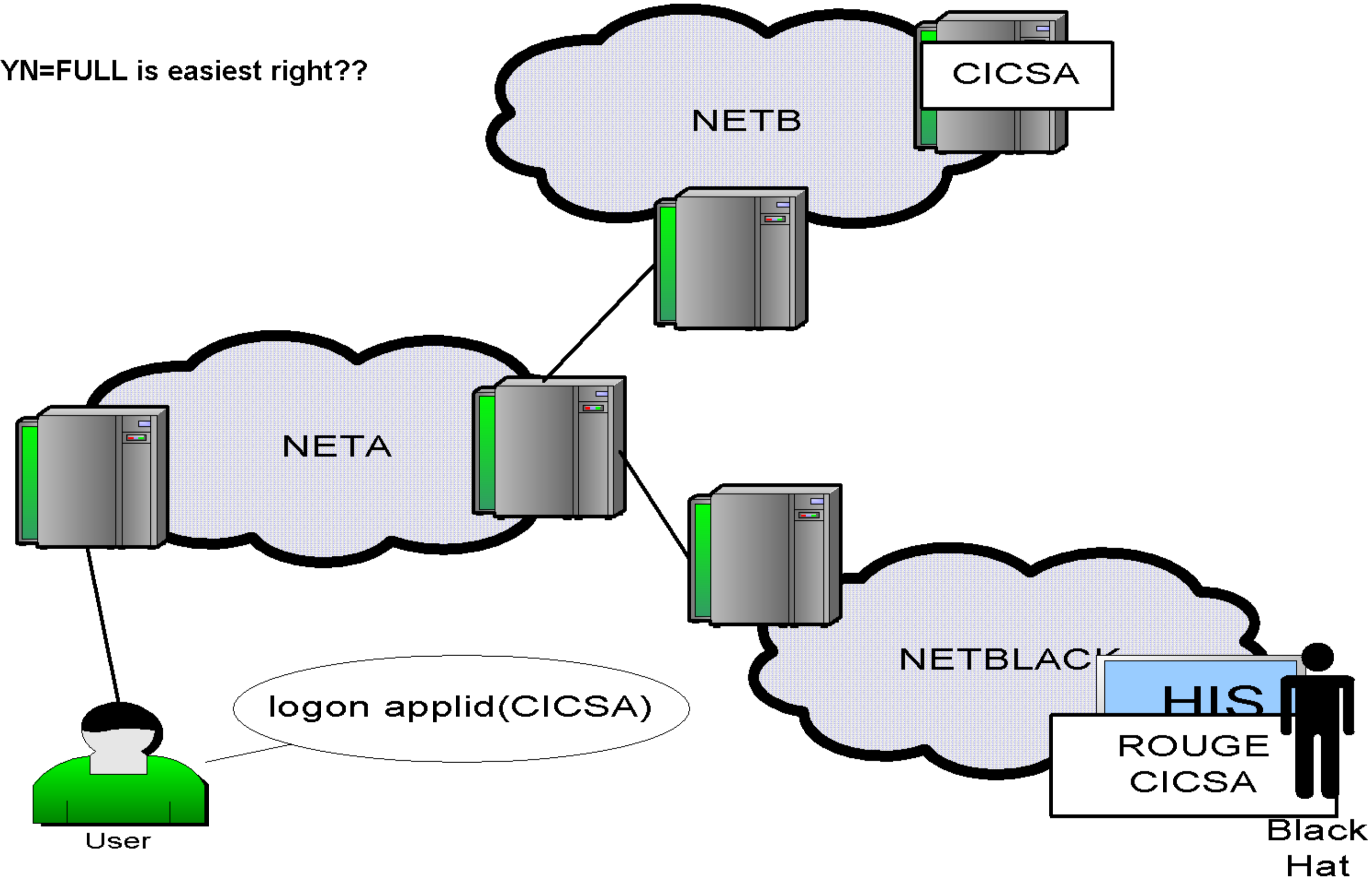
BNDYN Option

- **BNDYN=FULL**
  - Works all of the time
  - Searching is NOT optimized at all
  - Can result in a lot unnecessary searching (CPU and network overhead)
  - Adjacent subnetworks (including SNI) could see unnecessary searches too!
- **BNDYN=LIMITED**
  - Most "intelligent" searching option available
  - Works only for networks with very simple network interconnectivity
  - ALL resources must reside in immediately adjacent APPN subnetworks
  - No native resources with different NETIDs (SNI, LEN, EN or NNNA)
- **BNDYN=NONE**
  - Least "intelligent" searching option available
  - Requires ADJCLUST tables for EVERY possible target NETID (plus default table)
  - Will probably be needed by most customers who want optimal searching
- Again our best option for security in NONE since it will force the way a search will be preformed for a resource

© 2007 IBM Corporation

Example

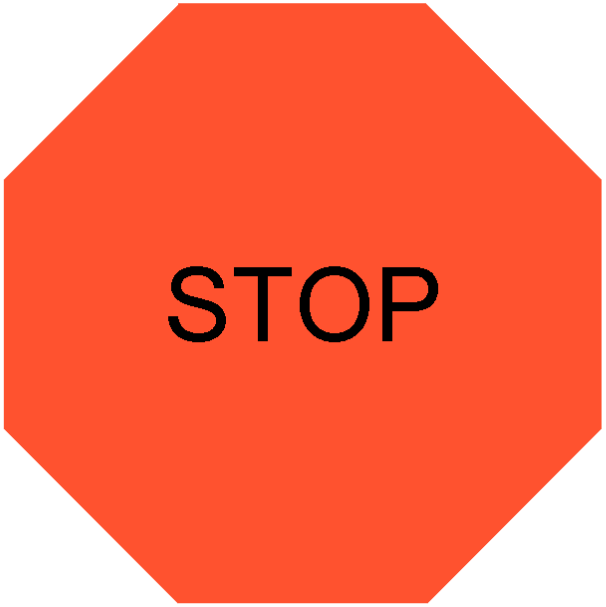
BNDYN=FULL is easiest right??



© 2007 IBM Corporation

BNDYN=NONE

Well if I just code BNDYN to NONE I should be safe then right????



“Not so fast my friend!!”

ADJClust Table

- **You have to construct your ADJCLUST table Correctly**

Here is an example of a bad ADJCLUST table….

```
**********************************************************************
SAMADJCL   VBUILD TYPE=ADJCLUST
**********************************************************************
* DEFAULT NETWORK ID
**********************************************************************
NONET         NETWORK  SNVC=4,            ALLOW DEPTH OF 4 NETWORKS    X
              BNDYN=LIMITED            ALLOW LIMITED DYNAMICS
ASYS2  NEXTCP    CPNAME=NETA.SYSA2
BSYS2  NEXTCP    CPNAME=NETB.SYSB2
CSYS2  NEXTCP    CPNAME=NETC.CSYC2
**********************************************************************
* ROUTING FOR NETID=NETB
**********************************************************************
NETB     NETWORK   NETID=NETB,                                         X
         BNDYN=LIMITED,                                                X
         SNVC=4                 ALLOW DEPTH OF 4 SUBNETS
BSYS2    NEXTCP    CPNAME=NETB.SYSB2
**********************************************************************
* ROUTING FOR NETID=NETB
**********************************************************************
NETC     NETWORK   NETID=NETC,                                         X
         BNDYN=LIMITED,                                                X
         SNVC=4                 ALLOW DEPTH OF 4 SUBNETS
CSYS2    NEXTCP    CPNAME=NETC.SYSC2
```

© 2007 IBM Corporation

A Better ADJCLUST table

```
********************************************************************************
SAMADJCL   VBUILD TYPE=ADJCLUST
********************************************************************************
* DEFAULT NETWORK ID
********************************************************************************
NONET         NETWORK   SNVC=1,              ALLOW DEPTH OF 1 NETWORKS        X
              BNDYN=NONE
ASYS2  NEXTCP    CPNAME=NETA.ASYS2
********************************************************************************
* ROUTING FOR NETID=NETB
********************************************************************************
NETB     NETWORK   NETID=NETB,                                               X
         BNDYN=NONE,                                                         X
         SNVC=2                 ALLOW DEPTH OF 1 SUBNETS
BSYS2    NEXTCP    CPNAME=NETB.BSYS2
********************************************************************************
* ROUTING FOR NETID=NETB
********************************************************************************
NETC     NETWORK   NETID=NETC,                                               X
         BNDYN=NONE,                                                         X
         SNVC=2                  ALLOW DEPTH OF 1 SUBNETS
CSYS2    NEXTCP    CPNAME=NETC.CSYS2
```

Extra Stuff!!!!

- **Depending on your Release you have some extra options you can use in the ADJCLUST table**
  - BNDYN can be overridden for each network definition
  - SNVC can be overridden for CP definition (Depth of search)

© 2007 IBM Corporation

Directory Services Management Exit

- **Called by Directory Services**
  - Called during search processing
  - Unlike the SME exit it has no awareness of sessions

- **DSME can be used for the following functions**
  - Boarder Node Selection
  - Authorization for an LU search
- **Example DSME code can be found on the z/OS communication support pages**

http://www-1.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=D400&uid=swg24014056&loc=en_US&cs=utf-8&lang=en

© 2007 IBM Corporation

Searches into a network

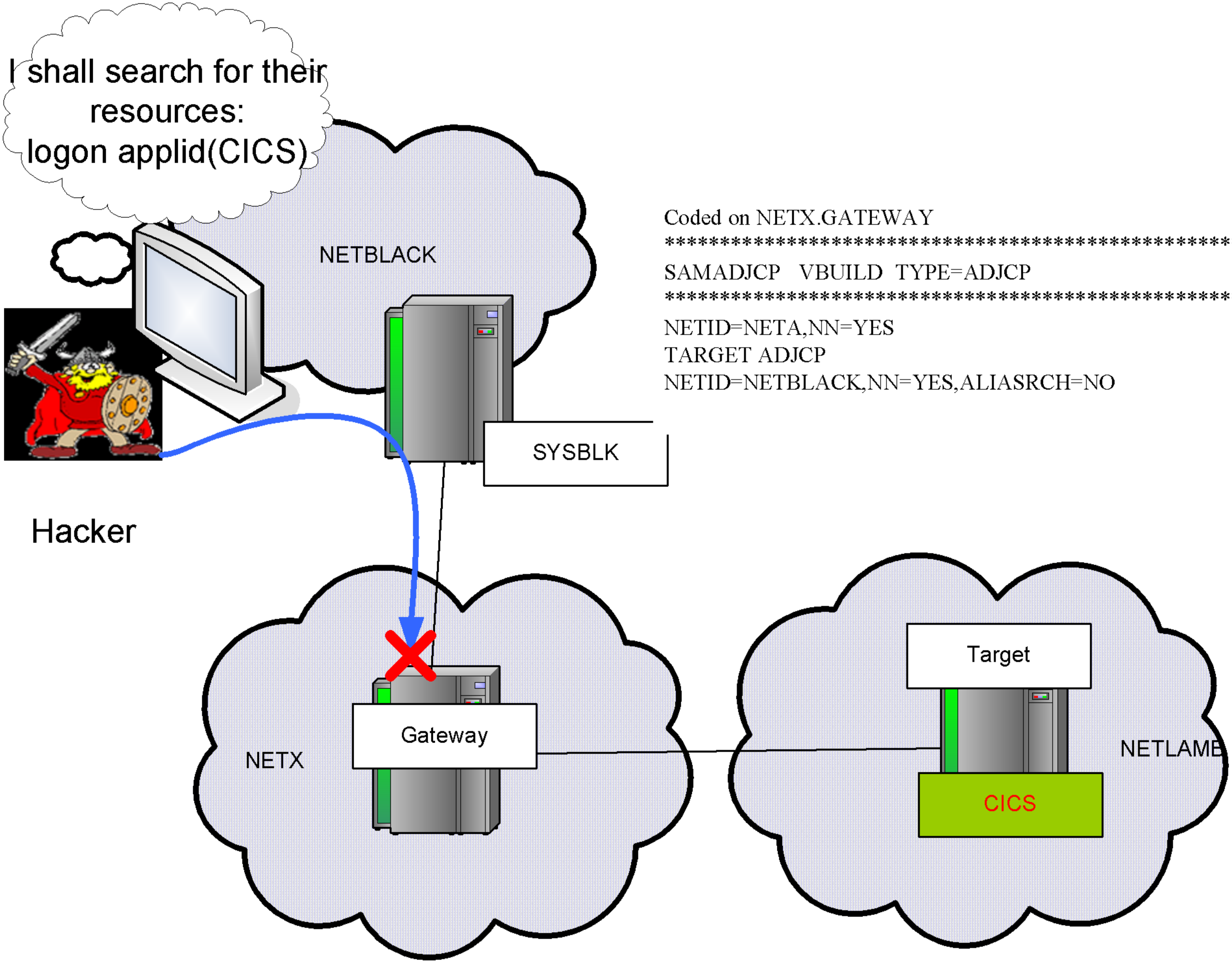
- **While we have shown ways of handling searches going out of the network it is also important to deal with searches entering the network**
- **Prior to V1R8 you would have to code a DSME exit to control this behavior**
- **However there have been advancements in VTAM to adopt some of the DSME function**

© 2007 IBM Corporation

Alias Searching

- Prior to V1R8 you could only restrict Alias Searching into the SNA network by coding a DSME exit
- In V1R8 a new option was added to the ADJCP definition.
- ALIASRCH can be used to prohibit non-network-qualified searches from coming into the network
- It is recommended that you code ALIASRCH=NO on all the Adjacent Control Points that are outside of the native network

© 2007 IBM Corporation

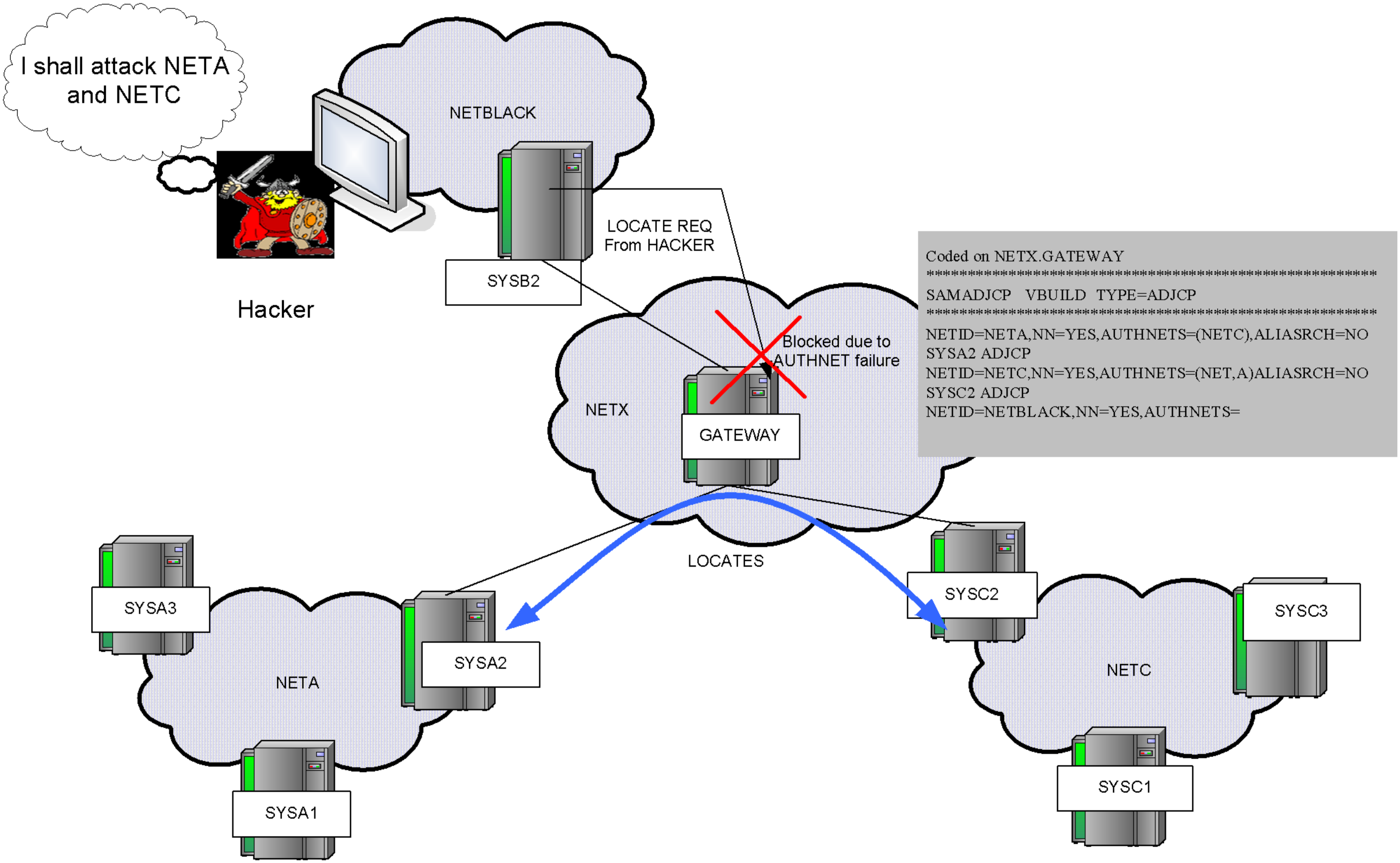


```
Coded on NETX.GATEWAY
*************************************************
SAMADJCP   VBUILD  TYPE=ADJCP
*************************************************
NETID=NETA,NN=YES
TARGET ADJCP
NETID=NETBLACK,NN=YES,ALIASRCH=NO
```

Authorizing Searches

- Prior to release V1R10 there was no way to prevent a fully qualified APPN search of another NETID from a non-Native NETID without a DSME exit
- In release V1R10 there will be a new option on the ADJCP definition called AUTHNETS
- Will allow an administrator to prevent searches of other Networks non-authorized CPs

© 2007 IBM Corporation



```
Coded on NETX.GATEWAY
************************************************************
SAMADJCP   VBUILD  TYPE=ADJCP
************************************************************
NETID=NETA,NN=YES,AUTHNETS=(NETC),ALIASRCH=NO
SYSA2 ADJCP
NETID=NETC,NN=YES,AUTHNETS=(NET,A)ALIASRCH=NO
SYSC2 ADJCP
NETID=NETBLACK,NN=YES,AUTHNETS=
```

Session Protection

- **While IPSec and TN3270 SSL/TLS can protect IP portions of a SNA data path; it does not protect the whole path**
- **Session Level Encryption (SLE)**
  - Allows for Data Confidentiality
    - DES (not recommended)
    - Triple DES (recommended)
  - Symmetric Keys
    - Held In SAF
    - Must be securely exchanged and refreshed on regular intervals
- **MAC Key word on the APPL definition**
  - Allows for Message Authentication
  - Setup very similar to SLE

© 2007 IBM Corporation

Conclusion

- **SNA networks are not going away**
- **The need to secure them is greater then ever**
- **Weave all 5 security areas together to protect your SNA Environment**
  - Physical Security
  - Network Security
  - Platform Security
  - Application Security
  - Policy Security
- **New White Paper: Securing an SNA Environment for the 21st Century**

http://www-1.ibm.com/support/docview.wss?rs=852&uid=swg27013237

- **More Security topics**

http://www-306.ibm.com/software/network/commserver/zos/security/

© 2007 IBM Corporation

For More Information....

URL	Content
http://www.ibm.com/systems/z/	IBM System z
http://www.ibm.com/systems/z/hardware/networking/index.html	IBM System z Networking
http://www.ibm.com/software/network/commserver/zos/	IBM z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	IBM Communications Server for Linux on zSeries
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library	IBM Communications Server Library - white papers, product documentation, etc.
http://www.redbooks.ibm.com	IBM Redbooks
http://www.ibm.com/software/network/commserver/support	IBM Communications Server Technical Support
http://www.ibm.com/support/techdocs/	Technical Support Documentation (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFCs)
http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp	IBM Education Assistant

© Copyright International Business Machines Corporation 2008. All rights reserved.

© 2007 IBM Corporation