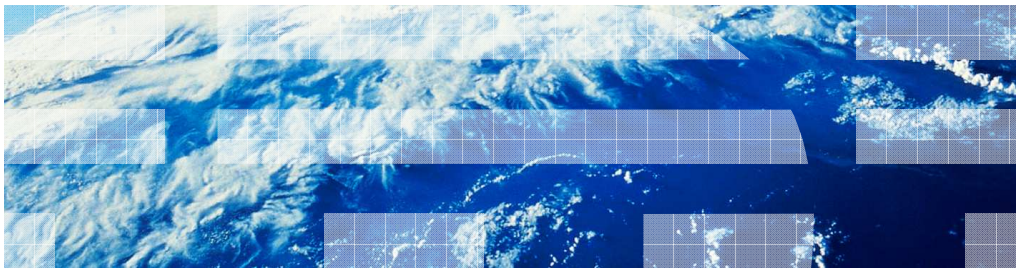
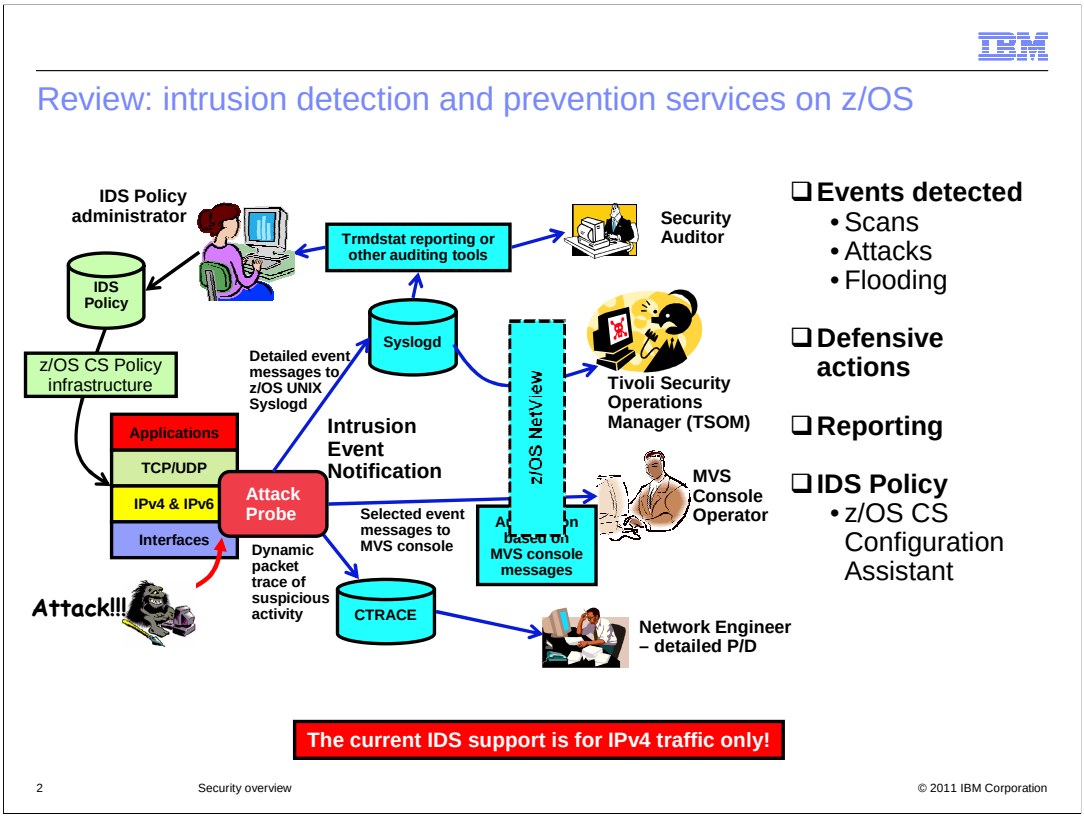
z/OS Communications Server – Security overview



This presentation provides an overview of the new functions in z/OS V1R13 Communications Server for security enhancements.



Intrusion detection services (IDS) supports detection of scans, attacks and flooding. IDS can be configured to discard packets or limit connections. Events can be logged to syslogd, to the MVS console, to IDS packet trace and to Tivoli Security Operations Manager (TSOM). IDS is configured using policy and is supported by the Configuration Assistant. Before z/OS V1R13, IDS is only supported for IPv4 traffic.

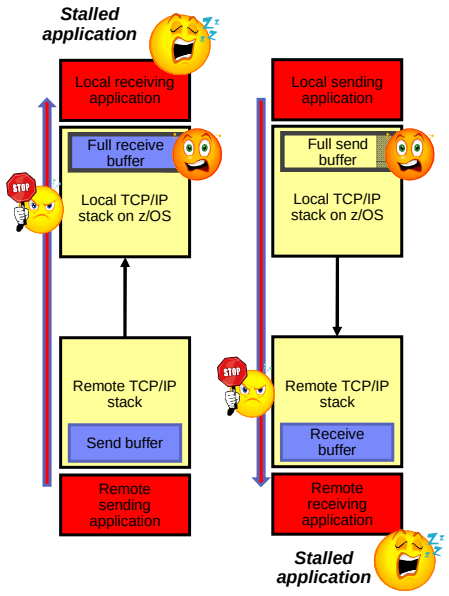
Intrusion detection services enhanced to include IPv6 traffic

- **Attack types supported for both IPv4 and IPv6**
  - Scan
  - Traffic regulation (TR)
  - Attack types extended to IPv6
  - Flood attacks
- **Plus, new attack types for IPv6-specific vulnerabilities**
  - Restricted IPv6 Next Header
  - Restricted IPv6 Hop Options
  - Restricted IPv6 Destination options
- **Note:** Defense Manager daemon already supports IPv6

In z/OS V1R13 Communications Server, the existing event detection for scans, traffic regulation, attacks and flood attacks is enhanced to include IPv6 traffic. TCP and UDP scan event rules now support IPv6 traffic. The ICMP scan event rule is unchanged and a corresponding ICMPv6 scan event rule is added. Scan exclusion lists can now include IPv6 addresses. TCP Traffic Regulation (TR) is enhanced to monitor IPv4 and IPv6 connection requests and UDP TR is enhanced to monitor IPv4 and IPv6 packets. The malformed packet event, UDP perpetual echo, and ICMP redirect restrictions attacks are extended to IPv6. IPv6 packets can be dropped due to malformed headers, options, or values. The SYN flood and interface flood attacks are extended to IPv6 as well. New attacks added for IPv6-specific vulnerabilities include Restricted IPv6 Next Header, Restricted IPv6 Hop Options, and Restricted IPv4 Destination options. The Defense Manager daemon already supports IPv6.

New IDS attack types implemented for both IPv4 and IPv6

- **Global TCP Stall**
  - Detects when a large number of TCP connections are stalled and unable to send data
- **Data Hiding**
  - Detects data hidden in reserved fields
- **TCP Queue Size**
  - Detects TCP send, receive, and out-of-order queues that are storage constrained



4 Security overview © 2011 IBM Corporation

In z/OS V1R13 Communications Server, IDS has implemented three new attack types for IPv4 and IPv6.

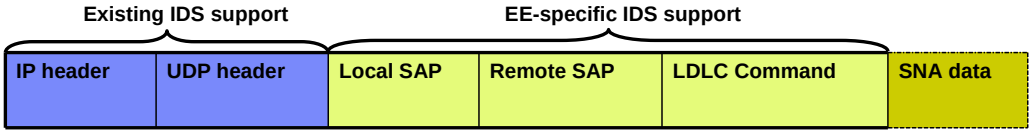
The global TCP stall attack type prevents an attacker from creating connections with zero window sizes and keeping them open indefinitely.

The data hiding attack type prevents an attacker from hiding data in reserved fields. This can be PadN options in IPv6 and reserved fields in IPv4 headers.

The TCP queue size attack type helps you manage the amount of storage TCP can take up for the queues holding sent and received data. For example, out of order packets awaiting re-sequencing. It provides user control over storage constraint availability improvements added in z/OS V1R11. This helps avoid TCP storage constraint situations.

Intrusion detection services for Enterprise Extender traffic

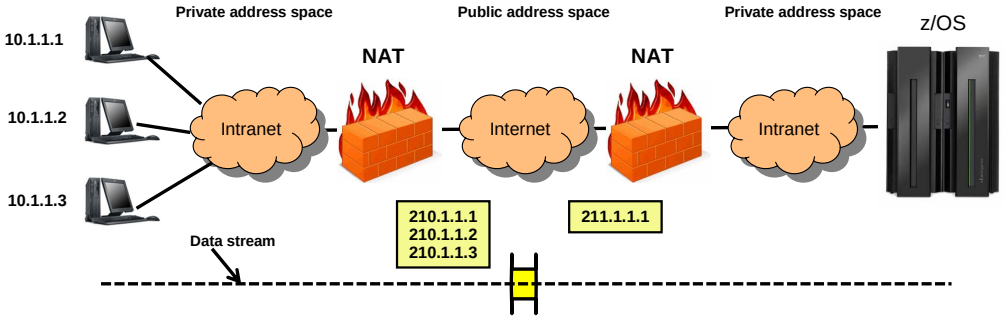
- Implement new EE-specific IDS attack types
  - EE Malformed Packet
  - EE LDLC Check
  - EE Port Check
  - EE XID Flood
- Exclusion list allowed for each attack type
- Actions are discard and notify
- IDS policy - z/OS CS Configuration Assistant
- IPv4 and IPv6



Intrusion detection services (IDS) is enhanced to implement four new IDS attack types for Enterprise Extender (EE). These attack types are supported for IPv4 and IPv6 EE traffic. The EE Malformed Packet attack type checks inbound EE packets for incorrect lengths. The EE LDLC Check attack type checks that inbound LDLC control commands are only received on the signaling port (12000). The EE Port Check attack type checks that inbound EE packets contain matching source and destination ports. The EE XID Flood attack type checks if a threshold is met for inbound XIDs within one minute. The actions allowed are to discard the packet and to provide a notification. The EE XID Flood attack only supports the notify action. An exclusion list can be created to exclude specific hosts from attack checking. Events notifications can be sent to syslogd, to the console, to IDS packet trace and to Tivoli Security Operations Manager (TSOM). IDS is configured using policies and is supported by the Configuration Assistant.

Support for network address translation when using IKEv2

- Network address translation (NAT) is commonly used in enterprises to conserve IPv4 addresses
- In z/OS V1R12, support was added for IKEv2, which was required for IPv6 currency
- Customers were encouraged to move to IKEv2, but for many, NAT is a requirement



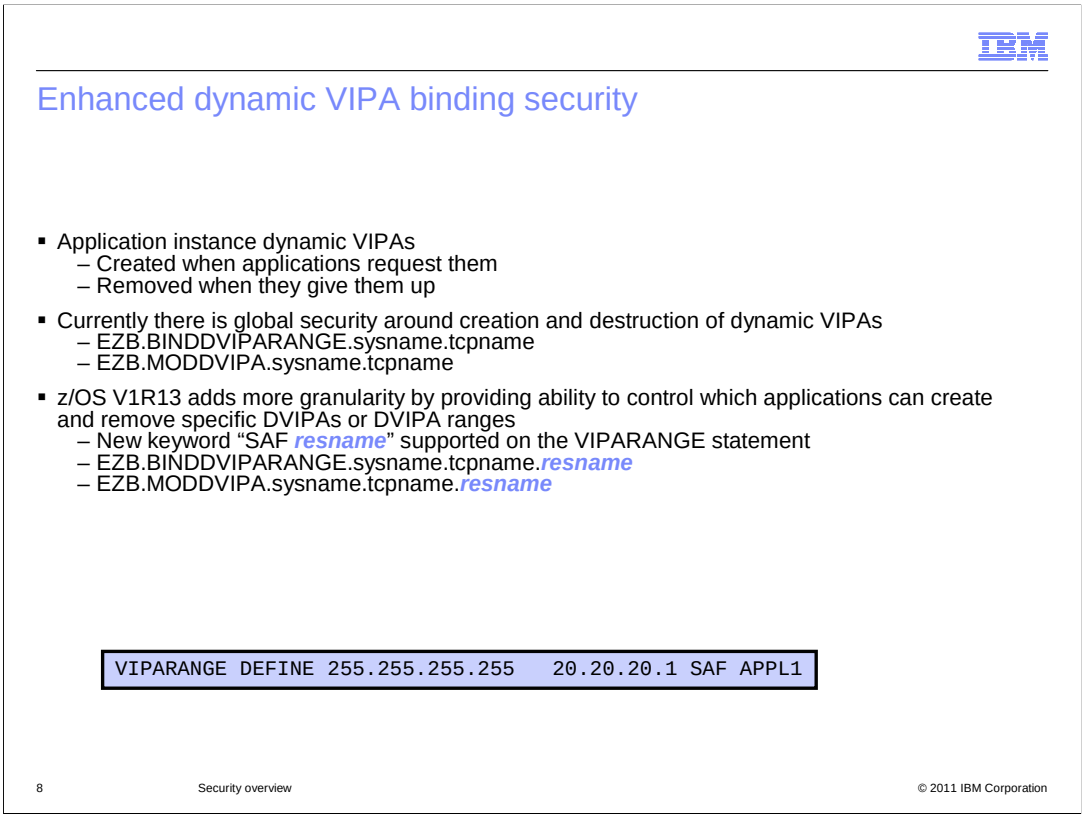
Network address translation (NAT) is commonly used to conserve IPv4 addresses. IKEv2 support was added in V1R12 and supports both IPv4 and IPv6.

In z/OS V1R13 Communications Server, NAT is now supported when using IKEv2. You can now migrate from IKEv1 to IKEv2 if you are using NAT.

Password phrase support in selected servers

- Password
  - One to eight characters
  - Limited range of characters allowed
- Password phrase
  - Nine to one hundred characters
  - Can contain most of the characters in the EBCDIC 1047code page
- Every user ID with a password phrase also has a password (since V1R10)
- Support for password phrases added to FTP and TN3270E in z/OS V1R13
  - TN3270E support is for solicitor screen only
    - Application password controls not affected

In z/OS V1R13 Communications Server, the FTP and TN3270E servers have been updated to support password phrases. Passwords are one to eight characters in length and have a limited range of characters allowed. For example, a space is not allowed in a password. Password phrases extend the length to 100 characters and support most of the characters in the 1047 code page.



Application instance dynamic VIPAs are virtual IP addresses that are created when applications request them and removed when they give them up. They provide improved availability. For example a dynamic VIPA can move around in the sysplex, following the application when it moves, so clients are uninterrupted.

Currently there is global security around creation and destruction of dynamic VIPAs. An application can be permitted to create and destroy all dynamic VIPAs. An application permitted to EZB.BINDDVIPARANGE.sysname.tcpname can bind to and remove all VIPARANGE defined DVIPAs. Similarly an application permitted to EZB.MODDVIPA.sysname.tcpname can issue MODDVIPA or SIOCSVIPA to create and remove all VIPARANGE defined DVIPAs.

z/OS V1R13 adds more granularity by providing ability to control which applications can create and remove specific DVIPAs or DVIPA ranges. This allows an application to create/remove its own DVIPAs but prevent it from interfering with other applications' ranges. A new keyword “SAF resname” is supported on the VIPARANGE statement. This identifies the resource profiles to use when creating or removing DVIPAs for the VIPARANGE statement. If the SAF keyword is not present, the existing profiles are used. In the example, to bind to 20.20.20.1, the application must be permitted to EZB.BINDDVIPARANGE.sysname.tcpname.APPL1 or to issue MODDVIPA 20.20.20.1, the application must be permitted to EZB.MODDVIPA.sysname.tcpname.APPL1.

Feedback

Your feedback is valuable

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

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

Click to send email feedback:

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

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

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

Trademarks, disclaimer, and copyright information